Web Application Security

Presented by:
Aidan Clarke

Field Systems Engineer
F5 Networks
a.clarke@f5.com

THE WORLD RUNS BETTER WITH F5

Why Security???

- The Internet is a scary place... (duh..)
- Criminals are not getting any dumber...
- There is money to be made...

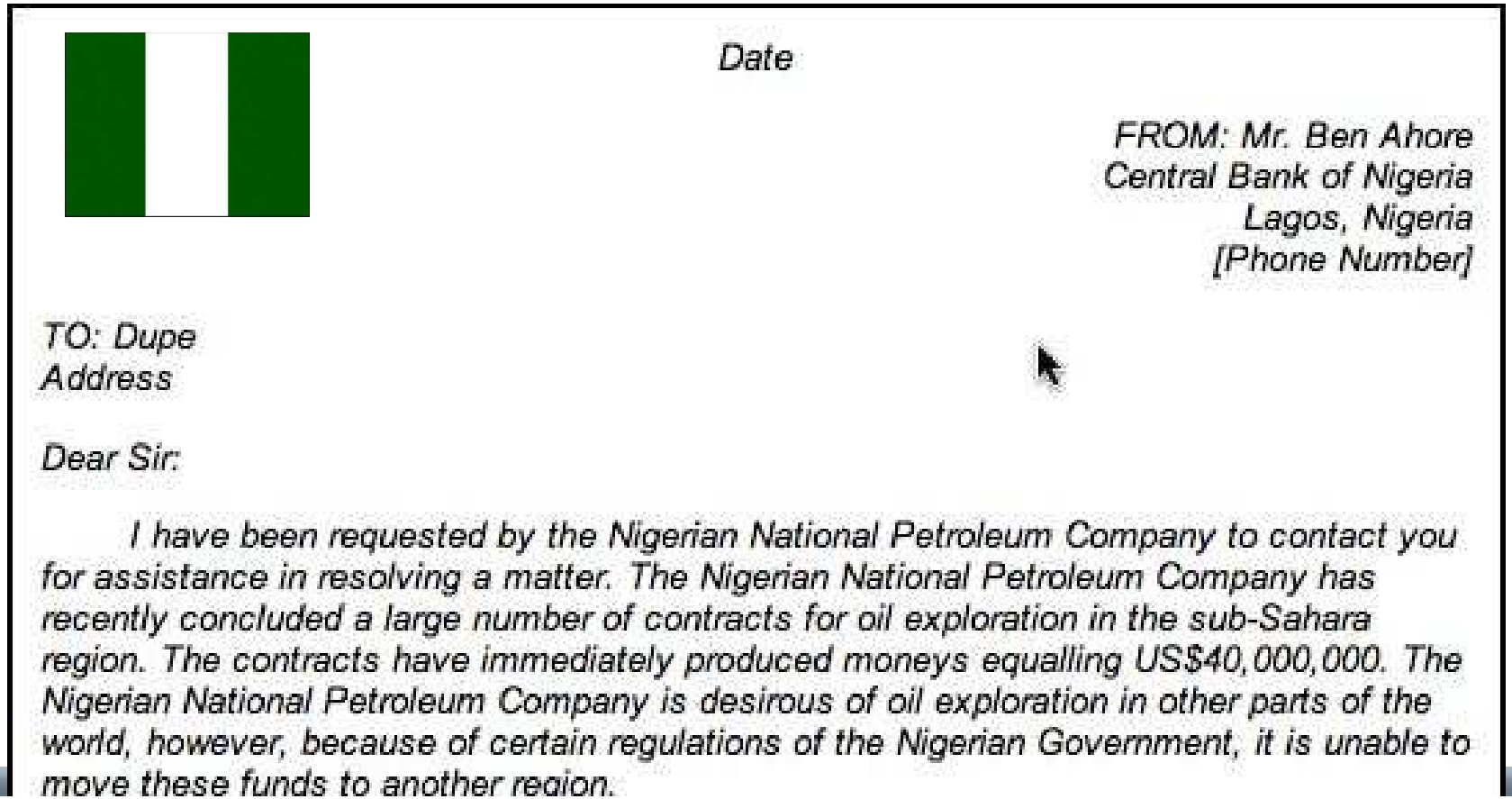
*** But you already knew this... Right? ***

- I won't tell you what you already know:

Security is *important*…

If you don't, then...

- I have an interesting investment opportunity to discuss with you after the session!



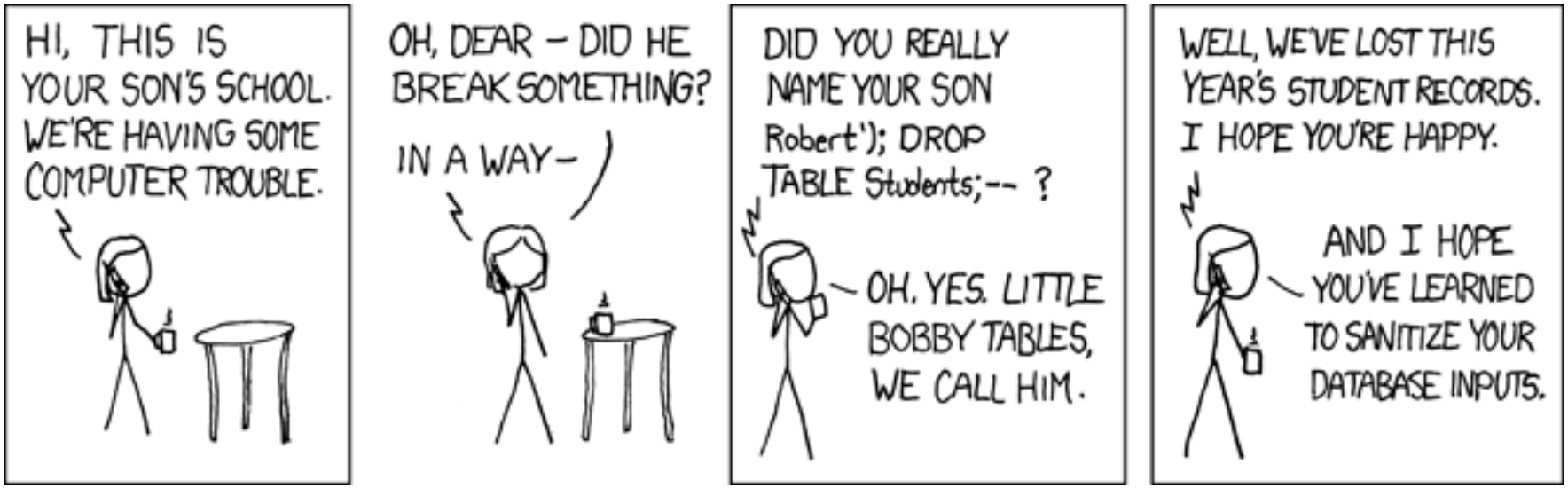
Date

FROM: Mr. Ben Ahore
Central Bank of Nigeria
Lagos, Nigeria
[Phone Number]

TO: Dupe
Address

Dear Sir:

I have been requested by the Nigerian National Petroleum Company to contact you for assistance in resolving a matter. The Nigerian National Petroleum Company has recently concluded a large number of contracts for oil exploration in the sub-Sahara region. The contracts have immediately produced moneys equalling US$40,000,000. The Nigerian National Petroleum Company is desirous of oil exploration in other parts of the world, however, because of certain regulations of the Nigerian Government, it is unable to move these funds to another region.


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

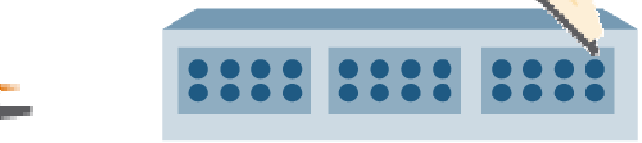
What are we here for this week?

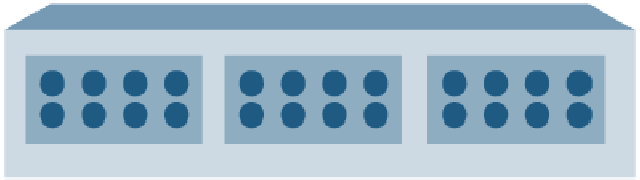
- To find out:
  - What are other people doing that I am not?
  - What tools are available to me that I did not know about?
  - How do I make it relevant to the business?
  - Where is the best place in my infrastructure to do it?
  - How do I sell it to the business?

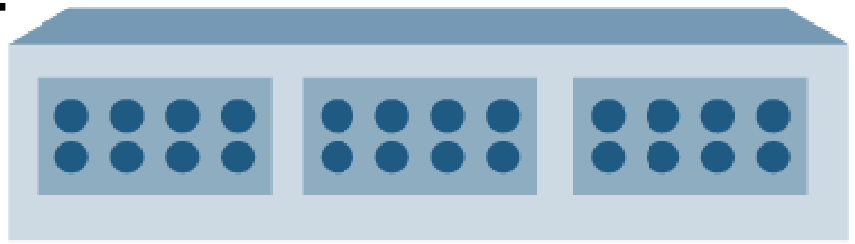
If only it were this easy…

3 Unique Sizes!

ALL NEW
Compliance ™ 2.0







IT SLICES, IT DICES,
IT CAN VACUUM YOUR BOAT
AND
DOUBLES AS AN OMELET MAKER!!!

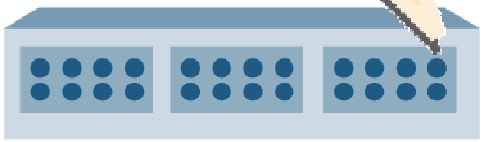
What you would really get…

3 Unique Sizes!

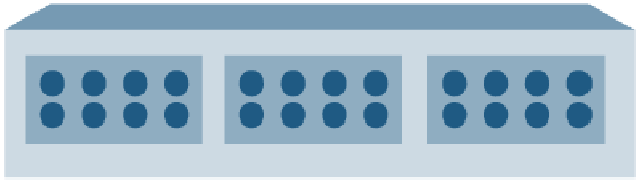
~~ALL NEW~~

REBADGED ACQUISITION

Compliance ™ Beta 0.1b

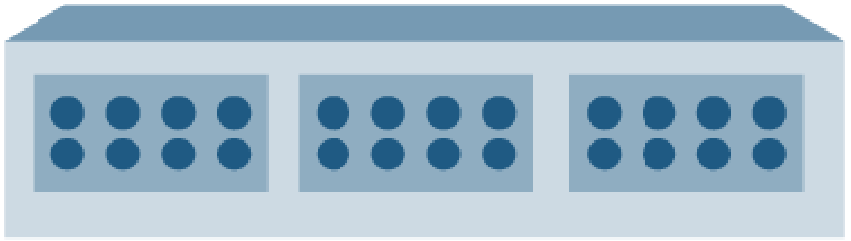


Small yet expensive



Medium and still very expensive

IT MAY SLICE, IT MIGHT DICE,
IT COULD ALMOST BE USED TO VACUUM YOUR BOAT,
CAUTION: WILL LIKELY RUIN YOUR EGGS NICELY…



Cabo here I come!!!

The Fine Print:

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc malesuada turpis quis tellus. Sed iaculis, eros nec porttitor nonummy, odio ligula lacinia ipsum, ut sagittis diam pede sit amet diam. Donec malesuada orci id diam. Fusce consectetuer bibendum ante. Integer suscipit massa lobortis arcu. In hac habitasse platea dictumst. Suspendisse suscipit. Nullam tincidunt. Nullam cursus dolor ut magna cursus ultrices. Nunc ligula. Ut dui mi, gravida eget, luctus in, convallis a, pede. Morbi id est id velit dignissim bibendum. Vestibulum consequat. Integer eu erat non turpis pulvinar semper.

Small print Cont…

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc malesuada turpis quis tellus. Sed iaculis, eros nec porttitor nonummy, odio ligula lacinia ipsum, ut sagittis diam pede sit amet diam. Donec malesuada orci id diam. Fusce consectetuer bibendum ante. Integer suscipit massa lobortis arcu. In hac habitasse platea dictumst. Suspendisse suscipit. Nullam tincidunt. Nullam cursus dolor ut magna cursus ultrices. Nunc ligula. Ut dui mi, gravida eget, luctus in, convallis a, pede. Morbi id est id velit dignissim bibendum. Vestibulum consequat. Integer eu erat non turpis pulvinar semper.

Proin ac nibh. Aenean vitae sapien. Integer commodo feugiat eros. In sit amet neque. Aenean tristique auctor tellus. Aliquam erat volutpat. Mauris non leo. Aliquam erat volutpat. Donec bibendum erat eget libero. Curabitur placerat, magna sit amet viverra lacinia, nibh leo ultricies velit, eu hendrerit felis nisi in nisi. Etiam quam. Fusce justo felis, fringilla quis, auctor a, vulputate id, urna. Mauris lectus lectus, scelerisque ut, pharetra sed, dictum eu, nisi. Phasellus bibendum vestibulum ipsum. Cras a augue.

Sed nec arcu vitae purus luctus tempor. Quisque euismod ligula ut neque. Maecenas in augue a mauris tempus adipiscing. Fusce tempus ullamcorper lacus. Praesent euismod. Donec sed dolor vestibulum augue porttitor fringilla. Nam lectus enim, porta vel, dignissim eu, sollicitudin non, ligula. Praesent eget nisi eget eros pellentesque feugiat. Proin non magna nec eros facilisis luctus. Integer gravida augue quis erat. Morbi vel felis vitae pede adipiscing adipiscing.

Nulla varius dui sed mi. Duis imperdiet lectus sit amet turpis. Morbi tortor nisi, rutrum ac, viverra eget, pellentesque volutpat, diam. Duis ullamcorper ipsum sit amet nibh. Donec neque odio, consequat sit amet, posuere vel, dignissim quis, mi. Integer rhoncus diam eu magna. Nam dictum. Cras sit amet pede. Aenean id massa. Morbi at dui eu est mattis sagittis. Fusce augue. Maecenas ante. Praesent vestibulum lacus quis nulla.

Phasellus sed eros. Aliquam ac velit. Cras ullamcorper, turpis vel blandit varius, mauris dui placerat leo, et pulvinar turpis justo eget purus. Duis massa neque, tincidunt ac, pulvinar nonummy, dapibus sed, dolor. Praesent aliquam, tellus elementum molestie volutpat, urna urna facilisis risus, sit amet iaculis pede nisi quis enim. Proin lectus est, imperdiet ac, tempus sit amet, consectetuer ut, elit. Aliquam erat volutpat. Curabitur lacus erat, aliquam vel, eleifend et, sagittis eget, lacus. Donec cursus ipsum. Duis velit arcu, lacinia at, semper eget, aliquet sed, turpis. Morbi sollicitudin elementum risus. Nunc tempor sagittis metus. Fusce elit lacus, lobortis sed, lacinia quis, vulputate a, nunc. Donec vel libero. Donec non magna sit amet sem ullamcorper dignissim. Curabitur sagittis augue eu felis. Morbi semper commodo metus. Quisque sagittis cursus erat. Vestibulum velit.

Praesent lobortis. Morbi eget neque sit amet lectus ornare gravida. Aenean ut elit quis ipsum fringilla sodales. Fusce imperdiet. Aenean eleifend laoreet justo. In dictum dapibus ante. Praesent rutrum est a neque. Praesent pharetra feugiat leo. Praesent vestibulum. Nam semper est ut ante. Aliquam erat volutpat. Aliquam convallis laoreet tortor. Sed urna. Pellentesque sagittis consectetuer libero. Nullam tempus fringilla elit. Sed metus erat, tempus rhoncus, fringilla ac, vulputate at, dolor. Maecenas blandit commodo tellus.

Pellentesque laoreet, sem sit amet elementum venenatis, orci sapien eleifend massa, sit amet dignissim orci quam nec pede. Curabitur lobortis metus a sem. Duis sit amet neque. Vestibulum mattis tempor diam. Nam convallis tristique nisi. Quisque tincidunt. Nulla commodo orci at magna. Aliquam fermentum cursus sapien. Ut dictum, urna id feugiat interdum, neque dolor ultricies arcu, at adipiscing odio dui vitae leo. Cras vitae lorem. Fusce pretium mi vel mi.

Etiam in nisi. Ut felis risus, tempus sed, tincidunt facilisis, vestibulum ut, mauris. Mauris tincidunt euismod tellus. Sed blandit. Suspendisse nec libero rhoncus metus luctus consectetuer. Ut suscipit convallis ligula. Donec pulvinar, mauris nec gravida lacinia, libero odio cursus erat, at convallis justo neque ut lectus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin viverra ante sed ante. Nunc a nisi. Proin pulvinar bibendum nunc. Pellentesque nec est. Morbi vulputate erat vel nisi. Donec iaculis ante eu nulla. Etiam vestibulum ante vel mi. Mauris sem nibh, dapibus sit amet, consequat ac, interdum sit amet, pede. Nullam egestas tortor sed ligula. Maecenas vulputate. Maecenas hendrerit, nulla sed feugiat consequat, nisl nisi cursus eros, vitae elementum massa quam vitae diam.

Integer in odio eu nulla egestas placerat. Morbi sed leo ac odio pharetra aliquet. Pellentesque a enim. Vestibulum purus. In suscipit. Aenean nulla tellus, semper non, rhoncus vel, porta ultrices, erat. Donec quis lorem non justo congue porttitor. Pellentesque hendrerit venenatis felis. In sed turpis eget metus sodales suscipit. Integer sed felis. Quisque ullamcorper, nunc non interdum luctus, odio libero vehicula mi, ac imperdiet purus velit volutpat purus. Nam et nulla non massa dapibus aliquam. In gravida diam eget sem viverra nonummy. Etiam ultrices neque id risus. Ut gravida. Cras tincidunt augue ut quam. Curabitur cursus. Aliquam quis odio euismod massa viverra posuere.

Aenean bibendum. Suspendisse et sem nec purus faucibus hendrerit. Curabitur et tortor. Quisque aliquam sapien a nibh. Mauris ut lacus sed odio commodo auctor. Nulla tempor. Morbi pellentesque. Donec massa. Etiam dictum sollicitudin diam. Mauris mattis rhoncus erat. Pellentesque pellentesque. Maecenas iaculis, velit eget placerat bibendum, pede nunc adipiscing arcu, non elementum mi ipsum vel purus. Phasellus feugiat diam. Sed viverra consequat nunc. Pellentesque vulputate egestas dui. Donec feugiat ullamcorper elit. Donec pharetra, neque sed interdum sollicitudin, mauris neque sodales odio, id sodales lorem ante in lorem. Sed mattis leo eu elit. Quisque posuere, leo gravida vestibulum blandit, ante lorem ultricies enim, sed rhoncus diam risus vel nulla. Suspendisse potenti.

Small print Cont… Cont…

Praesent lobortis. Morbi eget neque sit amet lectus ornare gravida. Aenean ut elit quis ipsum fringilla sodales. Fusce imperdiet. Aenean eleifend laoreet justo. In dictum dapibus ante. Praesent rutrum est a neque. Praesent pharetra feugiat leo. Praesent vestibulum. Nam semper est ut ante. Aliquam erat volutpat. Aliquam convallis laoreet tortor. Sed urna. Pellentesque sagittis consectetuer libero. Nullam tempus fringilla elit. Sed metus erat, tempus rhoncus, fringilla ac, vulputate at, dolor. Maecenas blandit commodo tellus.

Pellentesque laoreet, sem sit amet elementum venenatis, orci sapien eleifend massa, sit amet dignissim orci quam nec pede. Curabitur lobortis metus a sem. Duis sit amet neque. Vestibulum mattis tempor diam. Nam convallis tristique nisi. Quisque tincidunt. Nulla commodo orci at magna. Aliquam fermentum cursus sapien. Ut dictum, urna id feugiat interdum, neque dolor ultricies arcu, at adipiscing odio dui vitae leo. Cras vitae lorem. Fusce pretium mi vel mi.

Etiam in nisi. Ut felis risus, tempus sed, tincidunt facilisis, vestibulum ut, mauris. Mauris tincidunt euismod tellus. Sed blandit. Suspendisse nec libero rhoncus metus luctus consectetuer. Ut suscipit convallis ligula. Donec pulvinar, mauris nec gravida lacinia, libero odio cursus erat, at convallis justo neque ut lectus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin viverra ante sed ante. Nunc a nisi. Proin pulvinar bibendum nunc. Pellentesque nec est. Morbi vulputate erat vel nisi. Donec iaculis ante eu nulla. Etiam vestibulum ante vel mi. Mauris sem nibh, dapibus sit amet, consequat ac, interdum sit amet, pede. Nullam egestas tortor sed ligula. Maecenas vulputate. Maecenas hendrerit, nulla sed feugiat consequat, nisl nisi cursus eros, vitae elementum massa quam vitae diam.

Integer in odio eu nulla egestas placerat. Morbi sed leo ac odio pharetra aliquet. Pellentesque a enim. Vestibulum purus. In suscipit. Aenean nulla tellus, semper non, rhoncus vel, Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc malesuada turpis quis tellus. Sed iaculis, eros nec porttitor nonummy, odio ligula lacinia ipsum, ut sagittis diam pede sit amet diam. Donec malesuada orci id diam. Fusce consectetuer bibendum ante. Integer suscipit massa lobortis arcu. In hac habitasse platea dictumst. Suspendisse suscipit. Nullam tincidunt. Nullam cursus dolor ut magna cursus ultrices. Nunc ligula. Ut dui mi, gravida eget, luctus in, convallis a, pede. Morbi id est id velit dignissim bibendum. Vestibulum consequat. Integer eu erat non turpis pulvinar semper.

Proin ac nibh. Aenean vitae sapien. Integer commodo feugiat eros. In sit amet neque. Aenean tristique auctor tellus. Aliquam erat volutpat. Mauris non leo. Aliquam erat volutpat. Donec bibendum erat eget libero. Curabitur placerat, magna sit amet viverra lacinia, nibh leo ultricies velit, eu hendrerit felis nisi in nisi. Etiam quam. Fusce justo felis, fringilla quis, auctor a, vulputate id, urna. Mauris lectus lectus, scelerisque ut, pharetra sed, dictum eu, nisi. Phasellus bibendum vestibulum ipsum. Cras a augue.

Sed nec arcu vitae purus luctus tempor. Quisque euismod ligula ut neque. Maecenas in augue a mauris tempus adipiscing. Fusce tempus ullamcorper lacus. Praesent euismod. Donec sed dolor vestibulum augue porttitor fringilla. Nam lectus enim, porta vel, dignissim eu, sollicitudin non, ligula. Praesent eget nisi eget eros pellentesque feugiat. Proin non magna nec eros facilisis luctus. Integer gravida augue quis erat. Morbi vel felis vitae pede adipiscing adipiscing.

Nulla varius dui sed mi. Duis imperdiet lectus sit amet turpis. Morbi tortor nisi, rutrum ac, viverra eget, pellentesque volutpat, diam. Duis ullamcorper ipsum sit amet nibh. Donec neque odio, consequat sit amet, posuere vel, dignissim quis, mi. Integer rhoncus diam eu magna. Nam dictum. Cras sit amet pede. Aenean id massa. Morbi at dui eu est mattis sagittis. Fusce augue. Maecenas ante. Praesent vestibulum lacus quis nulla.

Phasellus sed eros. Aliquam ac velit. Cras ullamcorper, turpis vel blandit varius, mauris dui placerat leo, et pulvinar turpis justo eget purus. Duis massa neque, tincidunt ac, pulvinar nonummy, dapibus sed, dolor. Praesent aliquam, tellus elementum molestie volutpat, urna urna facilisis risus, sit amet iaculis pede nisi quis enim. Proin lectus est, imperdiet ac, tempus sit amet, consectetuer ut, elit. Aliquam erat volutpat. Curabitur lacus erat, aliquam vel, eleifend et, sagittis eget, lacus. Donec cursus ipsum. Duis velit arcu, lacinia at, semper eget, aliquet sed, turpis. Morbi sollicitudin elementum risus. Nunc tempor sagittis metus. Fusce elit lacus, lobortis sed, lacinia quis, vulputate a, nunc. Donec vel libero. Donec non magna sit amet sem ullamcorper dignissim. Curabitur sagittis augue eu felis. Morbi semper commodo metus. Quisque sagittis cursus erat. Vestibulum velit.

porta ultrices, erat. Donec quis lorem non justo congue porttitor. Pellentesque hendrerit venenatis felis. In sed turpis eget metus sodales suscipit. Integer sed felis. Quisque ullamcorper, nunc non interdum luctus, odio libero vehicula mi, ac imperdiet purus velit volutpat purus. Nam et nulla non massa dapibus aliquam. In gravida diam eget sem viverra nonummy. Etiam ultrices neque id risus. Ut gravida. Cras tincidunt augue ut quam. Curabitur cursus. Aliquam quis odio euismod massa viverra posuere.

Aenean bibendum. Suspendisse et sem nec purus faucibus hendrerit. Curabitur et tortor. Quisque aliquam sapien a nibh. Mauris ut lacus sed odio commodo auctor. Nulla tempor. Morbi pellentesque. Donec massa. Etiam dictum sollicitudin diam. Mauris mattis rhoncus erat. Pellentesque pellentesque. Maecenas iaculis, velit eget placerat bibendum, pede nunc adipiscing arcu, non elementum mi ipsum vel purus. Phasellus feugiat diam. Sed viverra consequat nunc. Pellentesque vulputate egestas dui. Donec feugiat ullamcorper elit. Donec pharetra, neque sed interdum sollicitudin, mauris neque sodales odio, id sodales lorem ante in lorem. Sed mattis leo eu elit. Quisque posuere, leo gravida vestibulum blandit, ante lorem ultricies enim, sed rhoncus diam risus vel nulla. Suspendisse potenti.

Small print Cont… Cont… Cont…

Nulla varius dui sed mi. Duis imperdiet lectus sit amet turpis. Morbi tortor nisi, rutrum ac, viverra eget, pellentesque volutpat, diam. Duis ullamcorper ipsum sit amet nibh. Donec neque odio, consequat sit amet, posuere vel, dignissim quis, mi. Integer rhoncus diam eu magna. Nam dictum. Cras sit amet pede. Aenean id massa. Morbi at dui eu est mattis sagittis. Fusce augue. Maecenas ante. Praesent vestibulum lacus quis nulla.

Phasellus sed eros. Aliquam ac velit. Cras ullamcorper, turpis vel blandit varius, mauris dui placerat leo, et pulvinar turpis justo eget purus. Duis massa neque, tincidunt ac, pulvinar nonummy, dapibus sed, dolor. Praesent aliquam, tellus elementum molestie volutpat, urna urna facilisis risus, sit amet iaculis pede nisi quis enim. Proin lectus est, imperdiet ac, tempus sit amet, consectetuer ut, elit. Aliquam erat volutpat. Curabitur lacus erat, aliquam vel, eleifend et, sagittis eget, lacus. Donec cursus ipsum. Duis velit arcu, lacinia at, semper eget, aliquet sed, turpis. Morbi sollicitudin elementum risus. Nunc tempor sagittis metus. Fusce elit lacus, lobortis sed, lacinia quis, vulputate a, nunc. Donec vel libero. Donec non magna sit amet sem ullamcorper dignissim. Curabitur sagittis augue eu felis. Morbi semper commodo metus. Quisque sagittis cursus erat. Vestibulum velit.

Praesent lobortis. Morbi eget neque sit amet lectus ornare gravida. Aenean ut elit quis ipsum fringilla sodales. Fusce imperdiet. Aenean eleifend laoreet justo. In dictum dapibus ante. Praesent rutrum est a neque. Praesent pharetra feugiat leo. Praesent vestibulum. Nam semper est ut ante. Aliquam erat volutpat. Aliquam convallis laoreet tortor. Sed urna. Pellentesque sagittis consectetuer libero. Nullam tempus fringilla elit. Sed metus erat, tempus rhoncus, fringilla ac, vulputate at, dolor. Maecenas blandit commodo tellus.

Pellentesque laoreet, sem sit amet elementum venenatis, orci sapien eleifend massa, sit amet dignissim orci quam nec pede. Curabitur lobortis metus a sem. Duis sit amet neque. Vestibulum mattis tempor diam. Nam convallis tristique nisi. Quisque tincidunt. Nulla commodo orci at magna. Aliquam fermentum cursus sapien. Ut dictum, urna id feugiat interdum, neque dolor ultricies arcu, at adipiscing odio dui vitae leo. Cras vitae lorem. Fusce pretium mi vel mi.

ante. Praesent rutrum est a neque. Praesent pharetra feugiat leo. Praesent vestibulum. Nam semper est ut ante. Aliquam erat volutpat. Aliquam convallis laoreet tortor. Sed urna. Pellentesque sagittis consectetuer libero. Nullam tempus fringilla elit. Sed metus erat, tempus rhoncus, fringilla ac, vulputate at, dolor. Maecenas blandit commodo tellus.

Pellentesque laoreet, sem sit amet elementum venenatis, orci sapien eleifend massa, sit amet dignissim orci quam nec pede. Curabitur lobortis metus a sem. Duis sit amet neque. Vestibulum mattis tempor diam. Nam convallis tristique nisi. Quisque tincidunt. Nulla commodo orci at magna. Aliquam fermentum cursus sapien. Ut dictum, urna id feugiat interdum, neque dolor ultricies arcu, at adipiscing odio dui vitae leo. Cras vitae lorem. Fusce pretium mi vel mi.

Etiam in nisi. Ut felis risus, tempus sed, tincidunt facilisis, vestibulum ut, mauris. Mauris tincidunt euismod tellus. Sed blandit. Suspendisse nec libero rhoncus metus luctus consectetuer. Ut suscipit convallis ligula. Donec pulvinar, mauris nec gravida lacinia, libero odio cursus erat, at convallis justo neque ut lectus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin viverra ante sed ante. Nunc a nisi. Proin pulvinar bibendum nunc. Pellentesque nec est. Morbi vulputate erat vel nisi. Donec iaculis ante eu nulla. Etiam vestibulum ante vel mi. Mauris sem nibh, dapibus sit amet, consequat ac, interdum sit amet, pede. Nullam egestas tortor sed ligula. Maecenas vulputate. Maecenas hendrerit, nulla sed feugiat consequat, nisl nisi cursus eros, vitae elementum massa quam vitae diam.

Integer in odio eu nulla egestas placerat. Morbi sed leo ac odio pharetra aliquet. Pellentesque a enim. Vestibulum purus. In suscipit. Aenean nulla tellus, semper non, rhoncus vel, porta ultrices, erat. Donec quis lorem non justo congue porttitor. Pellentesque hendrerit venenatis felis. In sed turpis eget metus sodales suscipit. Integer sed felis. Quisque ullamcorper, nunc non interdum luctus, odio libero vehicula mi, ac imperdiet purus velit volutpat purus. Nam et nulla non massa dapibus aliquam. In gravida diam eget sem viverra nonummy. Etiam ultrices neque id risus. Ut gravida. Cras tincidunt augue ut quam. Curabitur cursus. Aliquam quis odio euismod massa viverra posuere.

Aenean bibendum. Suspendisse et sem nec purus faucibus hendrerit. Curabitur et tortor. Quisque aliquam sapien a nibh. Mauris ut lacus sed odio commodo auctor. Nulla tempor. Morbi pellentesque. Donec massa. Etiam dictum sollicitudin diam. Mauris mattis rhoncus erat. Pellentesque pellentesque. Maecenas iaculis, velit eget placerat bibendum, pede nunc adipiscing arcu, non elementum mi ipsum vel purus. Phasellus feugiat diam. Sed viverra consequat nunc. Pellentesque vulputate egestas dui. Donec feugiat ullamcorper elit. Donec pharetra, neque sed interdum sollicitudin, mauris neque sodales odio, id sodales lorem ante in lorem. Sed mattis leo eu elit. Quisque posuere, leo gravida vestibulum blandit, ante lorem ultricies enim, sed rhoncus diam risus vel nulla. Suspendisse potenti.

Appliances will not save you…

- Security is about people and process: **tools can only help.**
  - You need the tools built in to your network.
- You can't throw the network out and start again,
  - Start small;
  - Scale or shift as business grows /requirements change...

You need flexible solutions that are not limited to what the vendors ***think*** you need.

Start with the basics...

- Security is managed risk:
  - Risk can be assessed and managed. Business does this every day...

- Understand what it is you are trying to protect:
  - Don’t expect people to spend $100 to secure a $0.50c problem;

Add security where there is value

- Keep security relevant to the business:
  - Without the business, there is nothing to secure...
- Plan for things to go wrong:
  - Sometimes you shouldn't say:

"I told you so"

Just be ready to dig them out...

Have a plan and the tools to dig the business out of trouble when it (invariably) comes...

Or someone else may end up digging a hole...

What are customers telling me?

- CFO / CIO pushing IT Dept to do MORE with LESS;
- PCI compliance is driving the application security push in *some* sectors.. (Others don't care!!);
- */(N|H)*I(D|P)S/ is mostly dead; but
- They still need the ability to respond to real threats / incidents dynamically;
- Most of all, Application Developers need room to BREATHE...

So lets drive your network harder...

- There are may areas where your network can be utilised to help your application:
  - Application Firewalls; and
  - Advanced Application Delivery Controllers.

- These are ideally placed to help ease the burden of application security on system integrators and developers.

What the hell is an AADC?

What the hell is an AADC?

- Application delivery controllers (ADCs) reside in the data center, typically in front of servers and are designed to improve the availability, performance and security of Web- or Internet Protocol-based applications.
- Advanced ADCs operate on a per-transaction basis and achieve application fluency. These devices become actively involved in the delivery of the application and provide sophisticated capabilities.

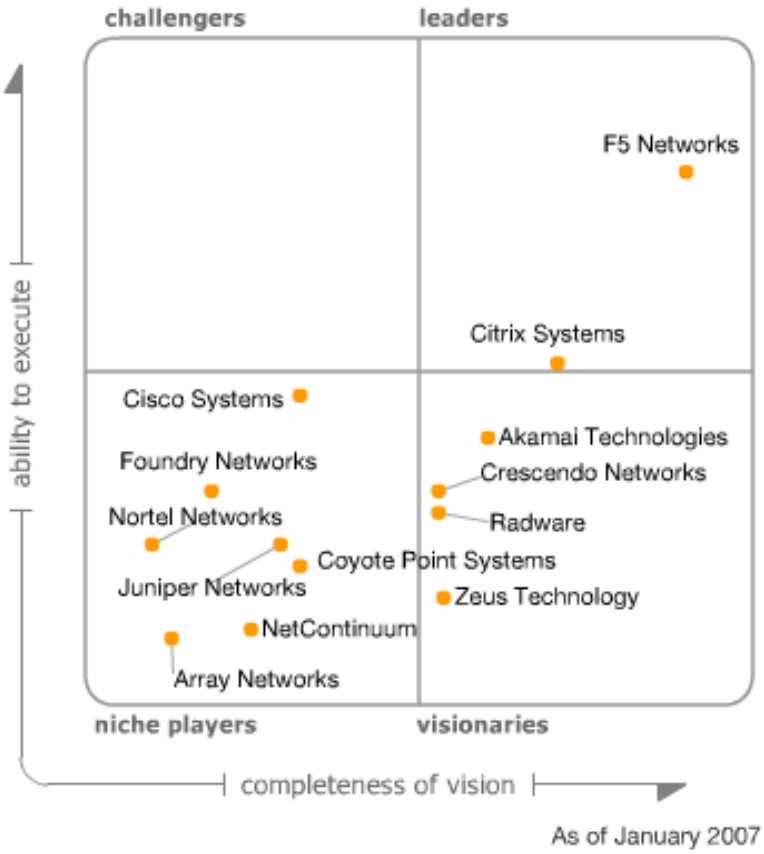
So what can they do?

- Application layer proxy, which is often bidirectional and stateful.
- Content transformation.
- Selective compression.
- Selective caching of dynamic content.
- HTML or other application protocol optimizations.
- Web application firewall.
- XML validation and transformation.
- Rules and programmatic interfaces.

So which tools are right for me?

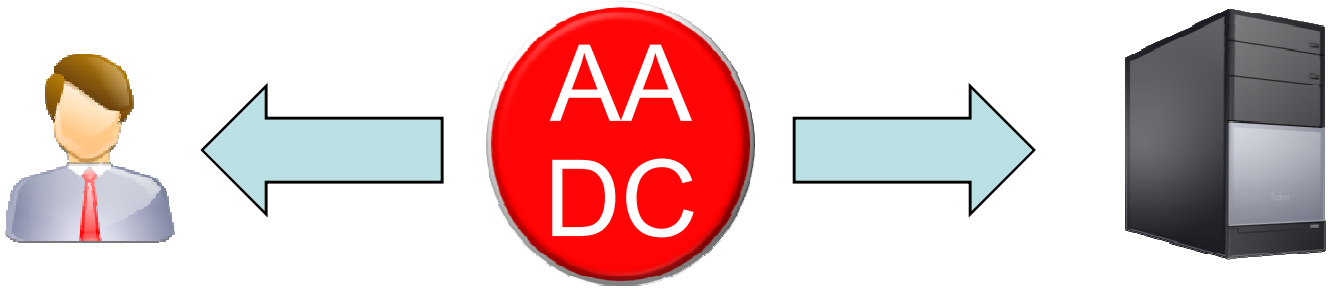
AADC Guidance – Gartner 2007

Gartner Magic Quadrant



What the hell do they do?

- Two key principles:
  - Access data in both directions;



  - Do *__SMART__* stuff based on that data;

Do you want to see what I mean?

Wouldn't it be cool if...

```
when HTTP_RESPONSE_DATA {
  # Find ALL the possible credit card numbers in one pass
  set card_indices [regexp -all -inline -indices {(?:30[0-
    5]\d{11})|(?:3[6|8]\d{12})|(?:3[4|7]\d{13})|(?:4\d{12})|(?:4\d{15})|(?:5[1-
    5]\d{14})|(?:6011\d{12})} [HTTP::payload]]


 # Calculate MOD10
    for { set i 0 } { $i < $card_len } { incr i } {
       set c [string index $card_number $i]
       if {($i & 1) == $double} {
          if {[incr c $c] >= 10} {incr c -9}
       }
       incr chksum $c
    }
```

Cool cont...

```
# If valid card number, then mask out numbers with
   X's
    if { ($chksum % 10) == 0 } {
       set isCard valid
       HTTP::payload replace $card_start $card_len
   [string repeat "X" $card_len]
    }
```

Web Application Firewalls

- Your Web Application Firewall needs to be able to do “Positive Security Policy”
- If you are relying on signature files for 0-day protection: **you will be 0wN3d...**
- Signatures should not be more than the 10% you do to prevent the *really* knuckleheaded stuff.

What should a WAF give me?

- Flexibility to do levels of security where you want it done...
  - Strict security for /login/ because it is important;
  - Basic security for /faq/ as it only hosts static content;
- Tools to facilitate policy building;
  - Learning mode it good;
  - Scriptable policy development / deployment code is better;
  - Both used together is a great thing to have...

Protect COTS apps that are stoopid...

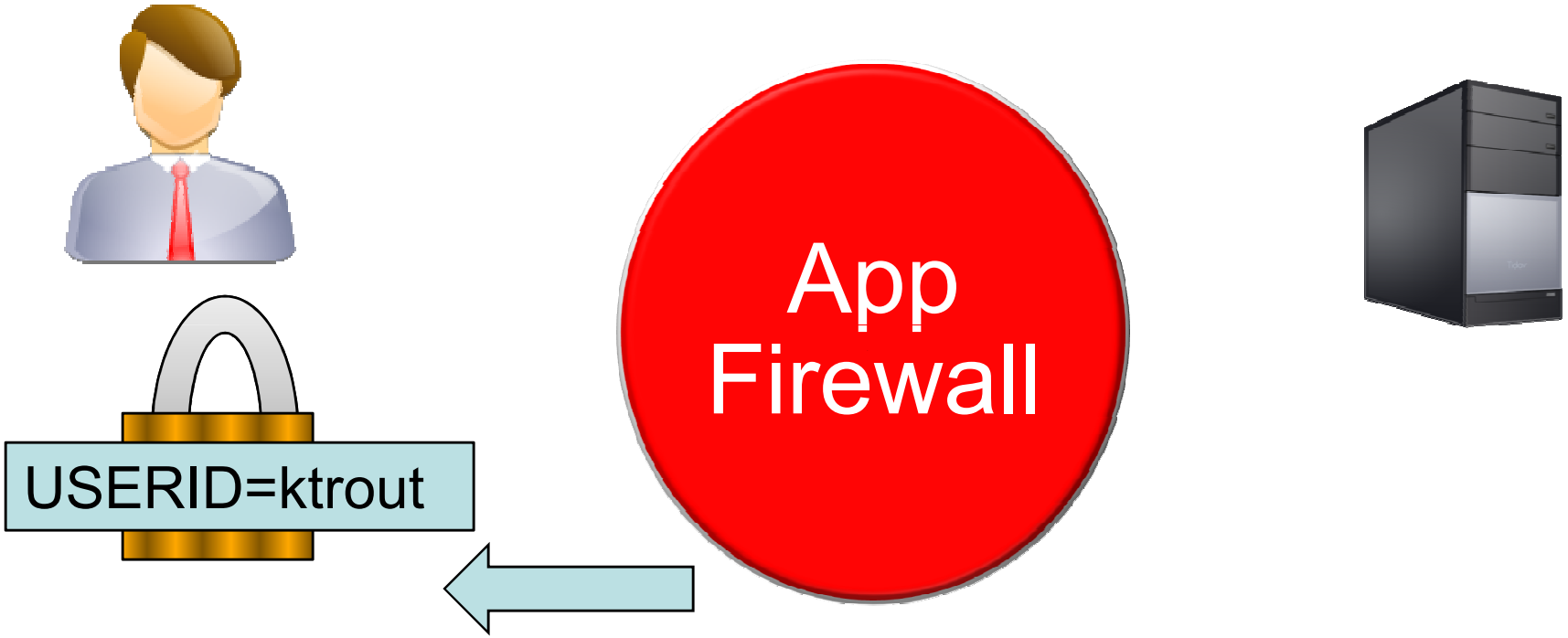
- <input type="hidden" name="userid" value="ktrout">
- <input type="hidden" name="credit_ok" value="1">
- <input type="hidden" name="form_expires" value="20001001:12:45:20">

Lets wrap some common sense around it...

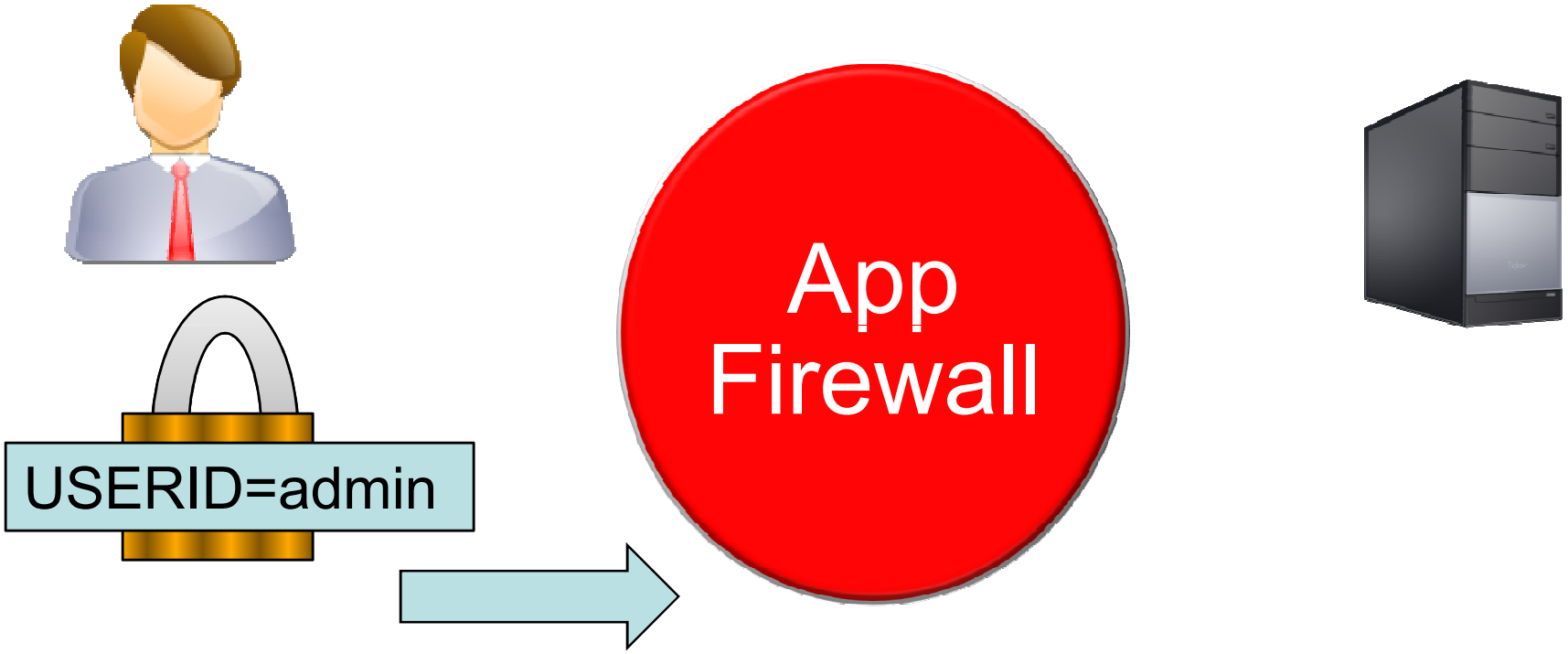
App Firewall

USERID=ktrout

Extract the hidden vars, and copy the values into an encrypted cookie



If the User changes the variable



It wont match the encrypted cookie value. We can discard the HTTP Transaction

USERID=ktrout

To block or not to block?

- Blocking Mode – Block violations against security policy;
- Transparent Mode – Alert, but do not block violations against security policy;
- Either way, ability to track just in case...

Logging & Reporting

- Make sure you understand what the logging and reporting you are getting;
- It needs to be tied into your incident response procedures;
- You ***DO*** have incident response procedures don't you?!?!

Questions?

THE WORLD RUNS BETTER WITH F5