Critical Stack

ADDRESSING SSL/TLS RISKS
WITH BRO

Presented by
Liam Randall

CONFIDENTIAL

This communication contains information that is confidential, proprietary in nature, and may also be attorney-client privileged and/or work product privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s) or the person responsible for delivering it to the intended recipient(s), please note that any form of dissemination, distribution or copying of this communication is strictly prohibited and may be unlawful. If you have received this communication in error, please immediately notify the sender and delete the original communication. Thank you for your cooperation.

PUBLIC SSL/TLS EXPLOITS

A failing web of trust…

Comodo

Adobe
APSA12-01

Microsoft
Flame

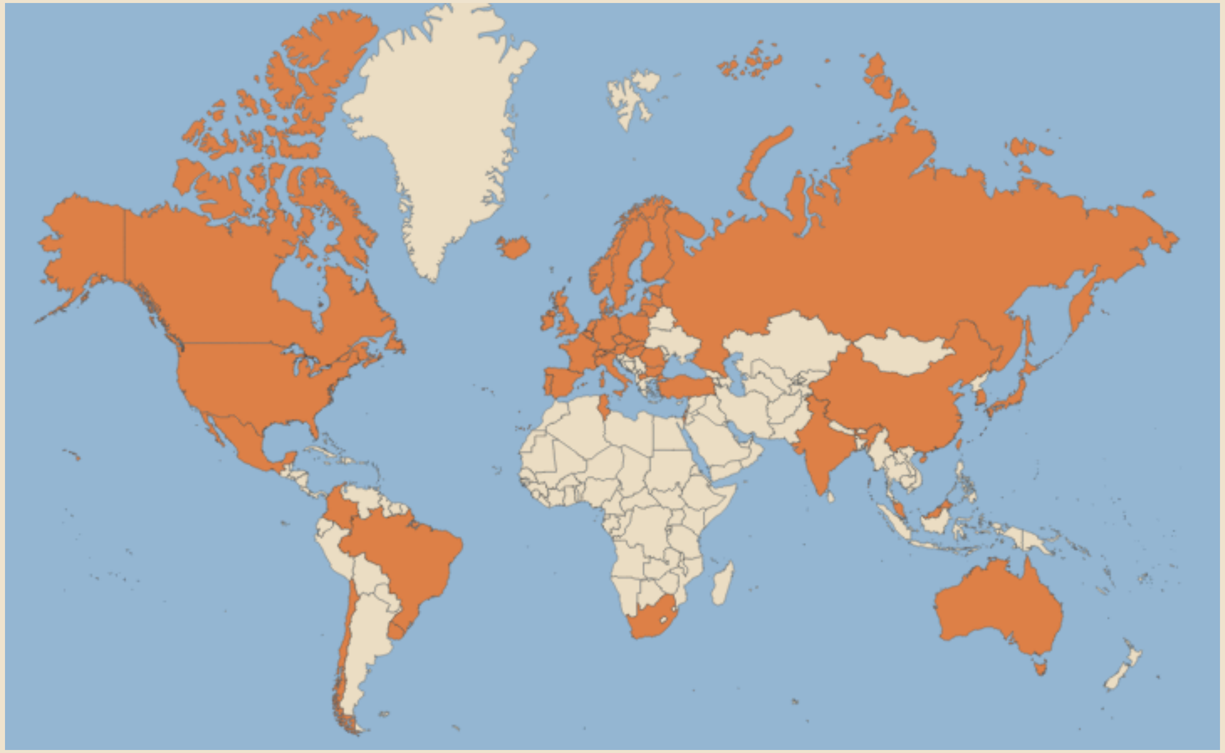
Fortigate
CVE-2012-4948

Cyberoam
CVE-2012-3372

DigiNotar

JURISDICTIONAL RISK

Distribution



Certificate Authority Entities

- 651 CA Organizations
- 52 Jurisdictions (Countries)
  - Many other Sub-CA

['AE', 'AT', 'AU', 'BE', 'BG', 'BM', 'BR', 'CA', 'CH', 'CL', 'CN', 'CO', 'CZ', 'DE', 'DK', 'EE', 'ES', 'EU', 'FI', 'FR', 'GB', 'HK', 'HU', 'IE', 'IL', 'IN', 'IS', 'IT', 'JP', 'KR', 'LT', 'LV', 'MK', 'MO','MX', 'MY', 'NL', 'NO', 'PL', 'PT', 'RO', 'RU', 'SE', 'SG', 'SI', 'SK', 'TN', 'TR', 'TW', 'UK', 'US', 'UY', 'WW', 'ZA']

Compiled by EFF SSL Observatory

PUBLIC SSL/TLS EXPLOITS

All 651 CA's can sign *everywhere* for *anything*.

The compromised companies are not the final target.

Comodo

Adobe
APSA12-01

Microsoft
Flame

Fortigate
CVE-2012-4948

Cyberoam
CVE-2012-3372

DigiNotar

NIST WARNING

ITL BULLETIN FOR JULY 2012

Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance

Paul Turner, Venafi

William Polk, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

1. Executive Summary

As the use of Public Key Infrastructure (PKI) and digital certificates (e.g., the use of Transport Layer Security [TLS] and Secure Sockets Layer [SSL]) for the security of systems has increased, the certification authorities (CAs) that issue certificates have increasingly become targets for sophisticated cyber-attacks. In 2011, several public certification authorities were attacked, and at least two attacks resulted in the successful issuance of fraudulent certificates by the attackers. An attacker who breaches a CA to generate and obtain fraudulent certificates does so to launch further attacks against other organizations or individuals. An attacker can also use fraudulent certificates to authenticate as another individual or system or to forge digital signatures.

These recent attacks on CAs make it imperative that organizations ensure they are using secure CAs and must also be prepared to respond to a CA compromise or issuance of a fraudulent certificate. Responding to a CA compromise may require replacing all user or device certificates or trust anchors.[1] If an organization is not prepared with an inventory of certificate locations and owners, the organization will not be able to respond in a timely manner and may experience significant interruption in its operations for an extended period of time. This document provides an overview of CA compromise and fraudulent certificate issuance scenarios and recommends steps for preparing for and responding to these incidents.

Many organizations have certificates issued from an external CA, and some organizations operate their own CAs. Nearly all organizations have users and/or systems that establish security using certificates belonging to the parties with whom they communicate. Since many of today's applications are sold with installed trust anchors that users may not be aware of or

[1] Relying parties use root certificates, referred to as trust anchors in this document, that they store locally to verify certificates they receive.

CA Compromises

"An attacker who breaches a CA to generate and obtain fraudulent certificates does so

to launch further attacks against other organizations or individuals."

http://csrc.nist.gov/publications/nistbul/july-2012_itl-bulletin.pdf

A TALE OF TWO CERT(IES)

When both valid, which CERT to Trust?

```
-----BEGIN CERTIFICATE-----
MIIDgDCCAumgAwIBAgIKGI35CwAAAAB4CzANBgkqhkiG9w0BAQUFADBGMQswCQYD
VQQGEwJVUzETMBEGA1UEChMKR29vZ2xlIEluYzEiMCAGA1UEAxMZR29vZ2xlIElu
dGVybmV0IEF1dGhvcml0eTAeFw0xMzAxMDMxMjE1NTJaFw0xMzA2MDcxOTQzMjda
MGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1N
b3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgSW5jMRcwFQYDVQQDEw53d3cu
Z29vZ2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAp0uFsoDllANv
ykrlbKlxgKFn97lG6Ca16b1ZT3vdGlBoxzrfcxXOqGkA1CcJqc3h0W4txqPpO9aq
lGODGmQnv/6HkNTmuOSJqHYjFRPgJ2s4CvofsexxCuw0/w2cHKfWRw/scGwqa4mQ
9d5Y6U6uTW/w8cp9csB6eZQo/oUBWMkCAwEAAaOCAVEwggFNMB0GA1UdJQQWMBQG
CCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUnkW9Yw+kcEJIu1VoSIQ8dwfb
6JQwHwYDVR0jBBgwFoAUv8Aw6/VDET5nup6R+/xq2uNrEiQwWwYDVR0fBFQwUjBQ
oE6gTIZKaHR0cDovL3d3dy5nc3RhdGljLmNvbS9Hb29nbGVJbnRlcm5ldEF1dGhv
cml0eS9Hb29nbGVJbnRlcm5ldEF1dGhvcml0eS5jcmwwZgYIKwYBBQUHAQEEWjBY
MFYGCCsGAQUFBzAChkpodHRwOi8vd3d3LmdzdGF0aWMuY29tL0dvb2dsZUludGVy
bmV0QXV0aG9yaXR5L0dvb2dsZUludGVybmV0QXV0aG9yaXR5LmNydDAMBgNVHRMB
Af8EAjAAMBkGA1UdEQQSMBCCDnd3dy5nb29nbGUuY29tMA0GCSqGSIb3DQEBBQUA
A4GBAFjwEoRMraJ+bM81lTrnT/qXXV1A2JwE+slBdVUysd4xAeg+yKnpxvfZ2H/i
AxELBVfQLO5R4f+Vr6axNFv4c8ne+FT4ZyNCEyD0sspESwhZXuXupc4ZMzm9xFa0
lxea+NUbP1EEgjiXkbtV6hcFVjFVgx7LsnSbuzp/SS418OFl

-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIFKDCCBBCgAwIBAgIQBeLmpM0J6lTWZbB1/iKiVjANBgkqhkiG9w0BAQUFADBm
MQswCQYDVQQGEwJOTDESMBAGA1UEChMJRGlnaU5vdGFyMSEwHwYDVQQDExhEaWdp
Tm90YXIgUHVibGljIENBIDIwMjUxIDAeBgkqhkiG9w0BCQEWEWluZm9AZGlnaW5v
dGFyLm5sMB4XDTExMDcxMDE5MDYzMFoXDTEzMDcwOTE5MDYzMFowajELMAkGA1UE
BhMCVVMxEzARBgNVBAoTCkdvb2dsZSBJbmMxFjAUBgNVBAcTDU1vdW50YWluIFZp
ZXcxFzAVBgNVBAUTDlBLMDAwMjI5MjAwMDAyMRUwEwYDVQQDEwwqLmdvb2dsZS5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDNbeKubCV0aCxhOiOS
CSQ/w9HXTYuD5BLKuiqXNw3setdTymeJz2L8aWOHo3nicFNDVwWTgwWomGNr2J6Q
7g1iINNSW0rR4E1l2szRkcnAY6c6i/Eke93nF4i2hDsnIBveolF5yjpuRm73uQQD
ulHjA3BFRF/PTi0fw2/Yt+8ieoMuNcMWN6Eou5Gqt5YZkWv176ofeCbsBmMrP87x
OhhtTDckCapk4VQZG2XrfzZcV6tdzCp5TI8uHdu17cdzXm1imZ8tyvzFeiCEOQN8
vPNzB/fIr3CJQ5q4uM5aKT3DD5PeVzf4rfJKQNgCTWiIBc9XcWEUuszwAsnmg7e2
EJRdAgMBAAGjggHMMIIByDA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0
dHA6Ly92YWxpZGF0aW9uLmRpZ2lub3Rhci5ubDAfBgNVHSMEGDAWgBTfM8Cvkv43
/LbYFhbQ2bGR1fpupTAJBgNVHRMEAjAAMIHGBgNVHSAEgb4wgbswgbgGDmCEEAGH
aQEBAQIEAQICMIGlMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2lub3Rhci5u
bC9jcHMwegYIKwYBBQUHAgIwbhpsQ29uZGl0aW9ucywgYXMgbWVudGlvbmVkIG9u
IG91ciB3ZWJzaXRlICh3d3cuZGlnaW5vdGFyLm5sKSwgYXJlIGFwcGxpY2FibGUg
dG8gYWxsIG91ciBwcm9kdWN0cyBhbmQgc2VydmljZXMuMEkGA1UdHwRCMEAwPqA8
oDqGOGh0dHA6Ly9zZXJ2aWNlLmRpZ2lub3Rhci5ubC9jcmwvcHVibGljMjAyNS9s
YXRlc3RDUkwuY3JsMA4GA1UdDwEB/wQEAwIEsDAbBgNVHREEFDASgRBhZG1pbkBn
b29nbGUuY29tMB0GA1UdDgQWBBQHSn0WJzIo0eMBMQUNsMqN6eF/7TANBgkqhkiG
9w0BAQUFAAOCAQEAAs5dL7N9wzRJkI4Aq4lC5t8j5ZadqnqUcgYLADzSv4ExytNH
UY2nH6iVTihC0UPSsILWraoeApdT7Rphz/8DLQEBRGdeKWAptNM3EbiXtQaZT2uB
pidL8UoafX0kch3f71Y1scpBEjvu5ZZLnjg0A8AL0tnsereOVdDpU98bKqdbbrnM
FRmBlSf7xdaNca6JJHeEpga4E9Ty683CmccrSGXdU2tTCuHEJww+iOAUtPIZcsum
```

BRO NETWORK SECURITY MONITOR

A TALE OF TWO CERT(IES)

When both valid, which CERT to Trust?

```
-----BEGIN CERTIFICATE-----
MIIDgDCCAumgAwIBAgIKGI35CwAAAAB4CzANBgkqhkiG9w0BAQUFADBGMQswCQYD
VQQGEwJVUzETMBEGA1UEChMKR29vZ2xlIEluYzEiMCAGA1UEAxMZR29vZ2xlIElu
dGVybmV0IEF1dGhvcml0eTAeFw0xMzAxMDMxMjE1NTJaFw0xMzA2MDcxOTQzMjda
MGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1N
b3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgSW5jMRcwFQYDVQQDEw53d3cu
Z29vZ2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAp0uFsoDllANv
ykrlbKlxgKFn97lG6Ca16b1ZT3vdGlBoxzrfcxXOqGkA1CcJqc3h0W4txqPpO9aq
lGODGmQnv/6HkNTmuOSJqHYjFRPgJ2s4CvofsexxCuw0/w2cHKfWRw/scGwqa4mQ
9d5Y6U6uTW/w8cp9csB6eZQo/oUBWMkCAwEAAaOCAVEwggFNMB0GA1UdJQQWMBQG
CCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUnkW9Yw+kcEJIu1VoSIQ8dwfb
6JQwHwYDVR0jBBgwFoAUv8Aw6/VDET5nup6R+/xq2uNrEiQwWwYDVR0fBFQwUjBQ
oE6gTIZKaHR0cDovL3d3dy5nc3RhdGljLmNvbS9Hb29nbGVJbnRlcm5ldEF1dGhv
cml0eS9Hb29nbGVJbnRlcm5ldEF1dGhvcml0eS5jcmwwZgYIKwYBBQUHAQEEWjBY
MFYGCCsGAQUFBzAChkpodHRwOi8vd3d3LmdzdGF0aWMuY29tL0dvb2dsZUludGVy
bmV0QXV0aG9yaXR5L0dvb2dsZUludGVybmV0QXV0aG9yaXR5LmNydDAMBgNVHRMB
Af8EAjAAMBkGA1UdEQQSMBCCDnd3dy5nb29nbGUuY29tMA0GCSqGSIb3DQEBBQUA
A4GBAFjwEoRMraJ+bM81lTrnT/qXXV1A2JwE+slBdVUysd4xAeg+yKnpxvfZ2H/i
AxELBVfQLO5R4f+Vr6axNFv4c8ne+FT4ZyNCEyD0sspESwhZXuXupc4ZMzm9xFa0
lxea+NUbP1EEgjiXkbtV6hcFVjFVgx7LsnSbuzp/SS418OFl
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIFKDCCBBCgAwIBAgIQBeLmpM0J6lTWZbB1/iKiVjANBgkqhkiG9w0BAQUFADBm
MQswCQYDVQQGEwJOTDESMBAGA1UEChMJRGlnaU5vdGFyMSEwHwYDVQQDExhEaWdp
Tm90YXIgUHVibGljIENBIDIwMjUxIDAeBgkqhkiG9w0BCQEWEWluZm9AZGlnaW5v
dGFyLm5sMB4XDTExMDcxMDE5MDYzMFoXDTEzMDcwOTE5MDYzMFowajELMAkGA1UE
BhMCVVMxEzARBgNVBAoTCkdvb2dsZSBJbmMxFjAUBgNVBAcTDU1vdW50YWluIFZp
ZXcxFzAVBgNVBAUTDlBLMDAwMjI5MjAwMDAyMRUwEwYDVQQDEwwqLmdvb2dsZS5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDNbeKubCV0aCxhOiOS
CSQ/w9HXTYuD5BLKuiqXNw3setdTymeJz2L8aWOHo3nicFNDVwWTgwWomGNr2J6Q
7g1iINNSW0rR4E1l2szRkcnAY6c6i/Eke93nF4i2hDsnIBveolF5yjpuRm73uQQD
ulHjA3BFRF/PTi0fw2/Yt+8ieoMuNcMWN6Eou5Gqt5YZkWv176ofeCbsBmMrP87x
OhhtTDckCapk4VQZG2XrfzZcV6tdzCp5TI8uHdu17cdzXm1imZ8tyvzFeiCEOQN8
vPNzB/fIr3CJQ5q4uM5aKT3DD5PeVzf4rfJKQNgCTWiIBc9XcWEUuszwAsnmg7e2
EJRdAgMBAAGjggHMMIIByDA6BggrBgEFBQcBAQQuMCwwKgYIKwYBBQUHMAGGHmh0
dHA6Ly92YWxpZGF0aW9uLmRpZ2lub3Rhci5ubDAfBgNVHSMEGDAWgBTfM8Cvkv43
/LbYFhbQ2bGR1fpupTAJBgNVHRMEAjAAMIHGBgNVHSAEgb4wgbswgbgGDmCEEAGH
aQEBAQIEAQICMIGlMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2lub3Rhci5u
bC9jcHMwegYIKwYBBQUHAgIwbhpsQ29uZGl0aW9ucywgYXMgbWVudGlvbmVkIG9u
IG91ciB3ZWJzaXRlICh3d3cuZGlnaW5vdGFyLm5sKSwgYXJlIGFwcGxpY2FibGUg
dG8gYWxsIG91ciBwcm9kdWN0cyBhbmQgc2VydmljZXMuMEkGA1UdHwRCMEAwPqA8
oDqGOGh0dHA6Ly9zZXJ2aWNlLmRpZ2lub3Rhci5ubC9jcmwvcHVibGljMjAyNS9s
YXRlc3RDUkwuY3JsMA4GA1UdDwEB/wQEAwIEsDAbBgNVHREEFDASgRBhZG1pbkBn
b29nbGUuY29tMB0GA1UdDgQWBBQHSn0WJzIo0eMBMQUNsMqN6eF/7TANBgkqhkiG
9w0BAQUFAAOCAQEAAs5dL7N9wzRJkI4Aq4lC5t8j5ZadqnqUcgYLADzSv4ExytNH
UY2nH6iVTihC0UPSsILWraoeApdT7Rphz/8DLQEBRGdeKWAptNM3EbiXtQaZT2uB
pidL8UoafX0kch3f71Y1scpBEjvu5ZZLnjg0A8AL0tnsereOVdDpU98bKqdbbrnM
FRmBlSf7xdaNca6JJHeEpga4E9Ty683CmccrSGXdU2tTCuHEJww+iOAUtPIZcsum
```

WEAK HASH

Known Attacks

- Additional risk Enterprises should control & monitor
- Collision Attacks

```
Risk factor :

Medium / CVSS Base Score : 4.0
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)
CVSS Temporal Score : 3.3
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true
```

Replace Immediately

- MD2
- MD4
- MD5

MITIGATIONS EFFORTS

Well known problem

CMU Perspectives

- Browser Based

Certificate Patrol

- Browser Based
- Notify on Updates

convergence.io

- Browser Based
- Distributed Trust

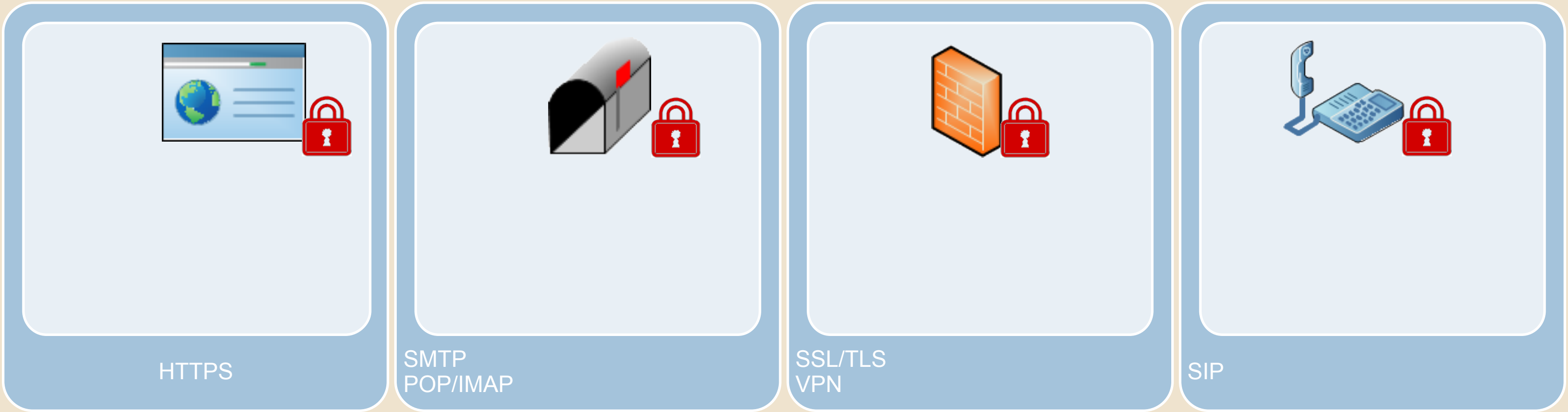
ICSI SSL Notary

- DNS Lookups

AFFECTED SERVICES

Example Use Cases

- + Credit Checks
- + Authorization and Accounting
- + Supply Chain Management
- + e-Commerce
- + Marketing

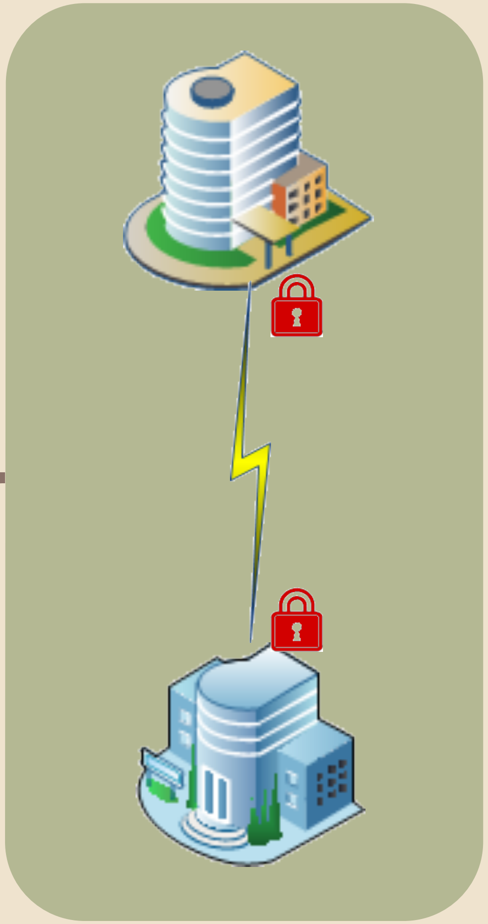


HTTPS

SMTP
POP/IMAP

SSL/TLS
VPN

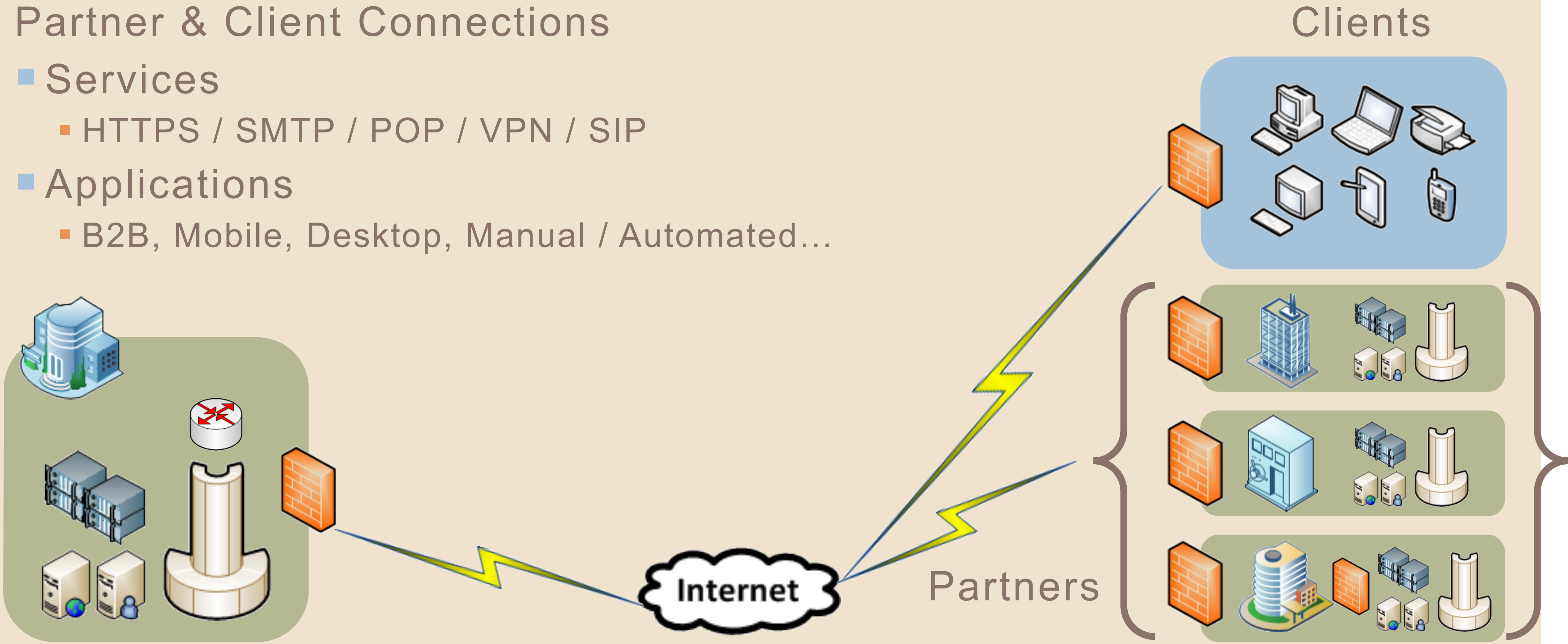
SIP



B2B WHAT SHOULD WE KNOW

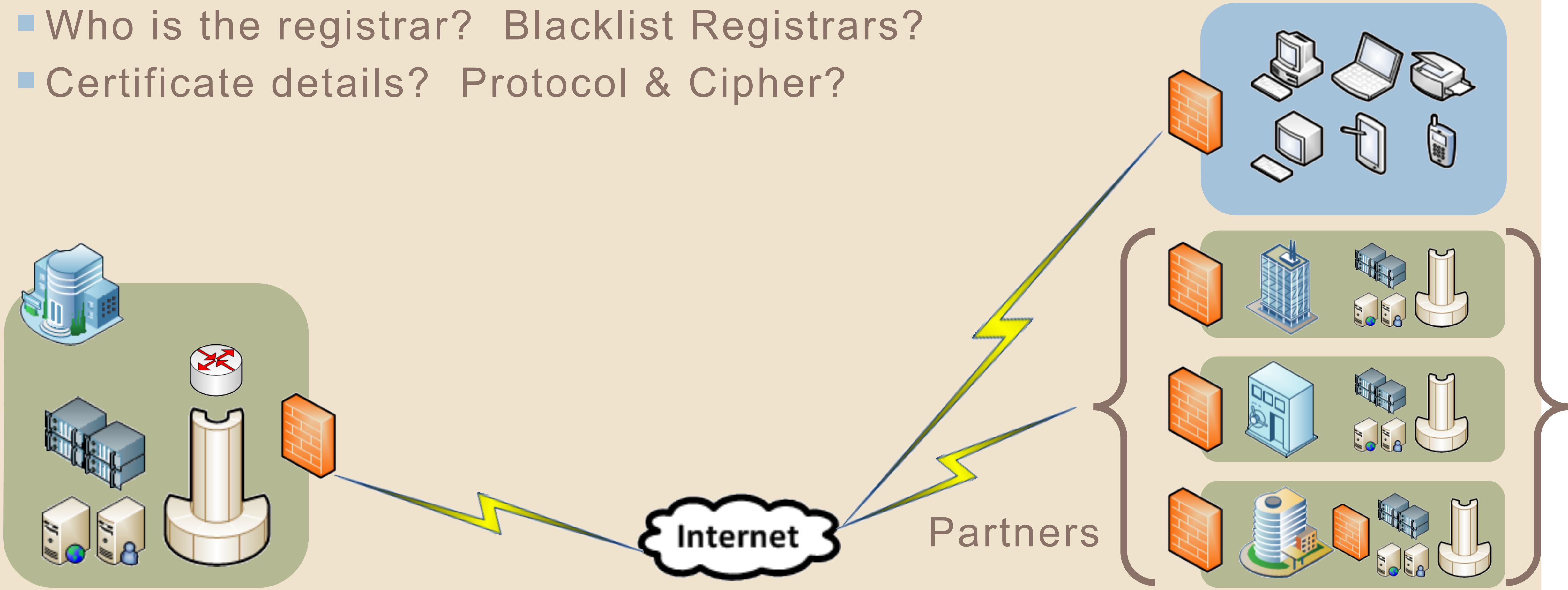
Partner & Client Connections

- Services
  - HTTPS / SMTP / POP / VPN / SIP
- Applications
  - B2B, Mobile, Desktop, Manual / Automated…



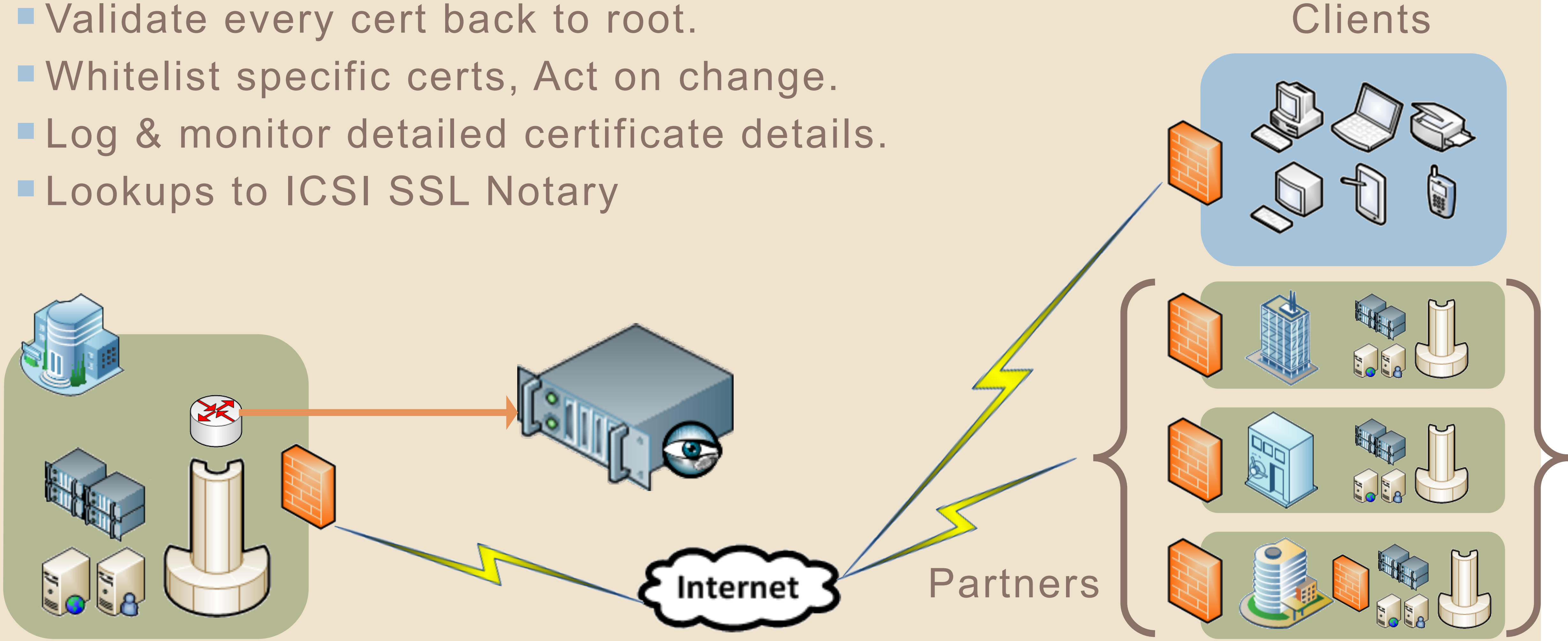
B2B SSL/TLS IOC

- When do certs change? Expire?
- Who is the registrar? Blacklist Registrars?
- Certificate details? Protocol & Cipher?



BRO INSIGHTS

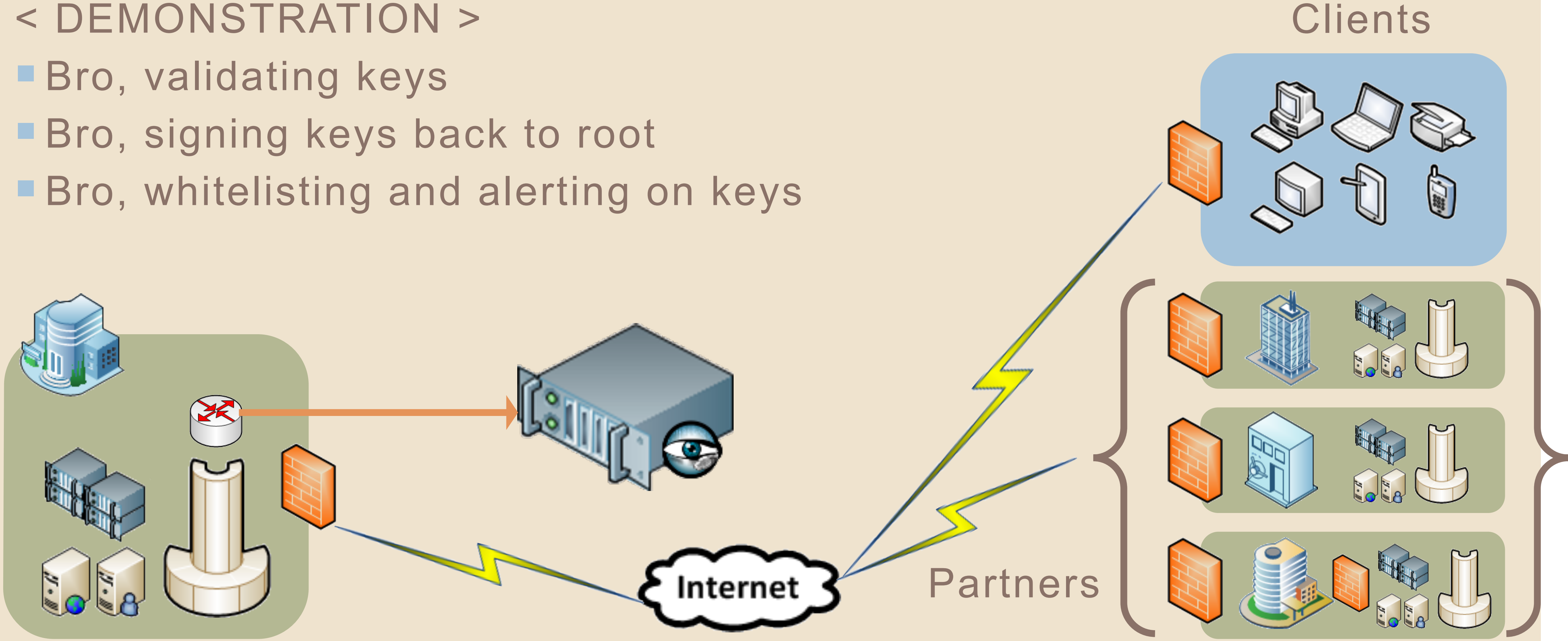
- Validate every cert back to root.
- Whitelist specific certs, Act on change.
- Log & monitor detailed certificate details.
- Lookups to ICSI SSL Notary



BRO INSIGHTS

< DEMONSTRATION >

- Bro, validating keys
- Bro, signing keys back to root
- Bro, whitelisting and alerting on keys


Clients
Internet
Partners