



Webinaire sur la sécurité du serveur IceWarp

15 octobre 2009

La sécurité

Les vulnérabilités

SMTP
POP
IMAP
HTTP
...



Les risques

Saturation du serveur
Saturation des réseaux
Mise en liste noire par les serveurs distants
Intégrité du serveur
Ecoute et corruption des données

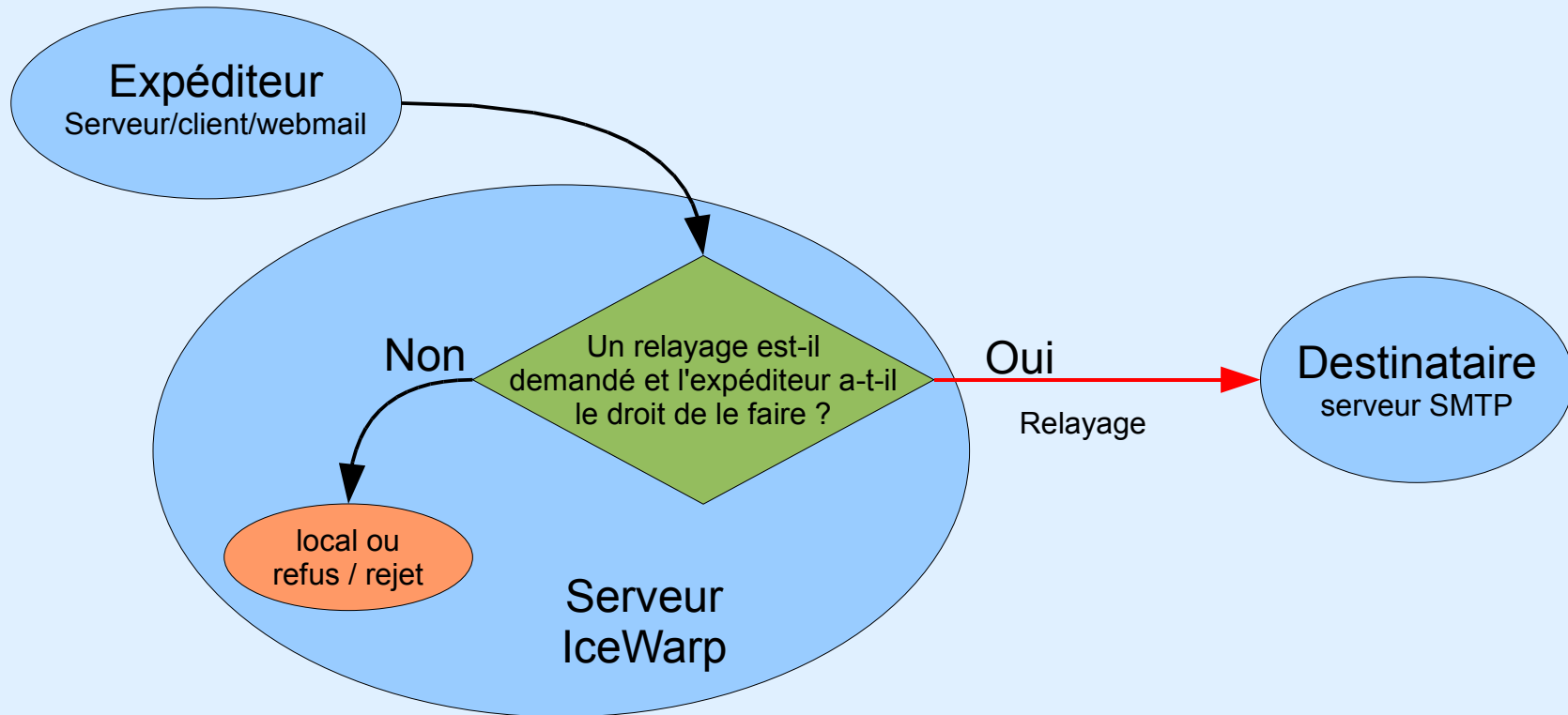


Les protections



Le contrôle du relayage
L'authentification
Le cryptage
L'architecture
L'anti virus
L'anti Spam

Le flux de relayage



" will forward "

```
41.202.24.147 [0DF4] 15:48:46 Connected
41.202.24.147 [0DF4] 15:48:46 >>> 220 smtp.domaine.fr ESMTP IceWarp 9.3.2; Mon, 07 Sep 2009 15:48:...
41.202.24.147 [0DF4] 15:48:46 <<< EHLO User
41.202.24.147 [0DF4] 15:48:46 >>> 250-smtp.domaine.fr Hello User [41.202.24.147], pleased to meet you.
41.202.24.147 [0DF4] 15:48:47 <<< AUTH LOGIN
41.202.24.147 [0DF4] 15:48:47 >>> 334 VXNlcm5hbWU6
41.202.24.147 [0DF4] 15:48:47 <<< dGVzdA==
41.202.24.147 [0DF4] 15:48:47 >>> 334 UGFzc3dvcmQ6
41.202.24.147 [0DF4] 15:48:47 <<< dGVzdA==
41.202.24.147 [0DF4] 15:48:47 >>> 235 2.0.0 Authentication successful
41.202.24.147 [0DF4] 15:48:47 <<< RSET
41.202.24.147 [0DF4] 15:48:47 >>> 250 2.0.0 Reset state
41.202.24.147 [0DF4] 15:48:47 <<< MAIL FROM:<mr.luckywilliams.gh1@gmail.com>
41.202.24.147 [0DF4] 15:48:47 >>> 250 2.1.0 <mr.luckywilliams.gh1@gmail.com>... Sender ok
41.202.24.147 [0DF4] 15:48:47 <<< RCPT TO:<alwis@trc.gov.lk>
41.202.24.147 [0DF4] 15:48:47 >>> 250 2.1.5 <alwis@trc.gov.lk>... Recipient ok; will forward
41.202.24.147 [0DF4] 15:48:48 <<< RCPT TO:<aly@myownemail.com>
```

Site de décodage de base64 :

<http://www.themanualpage.org/utills/base64.php>

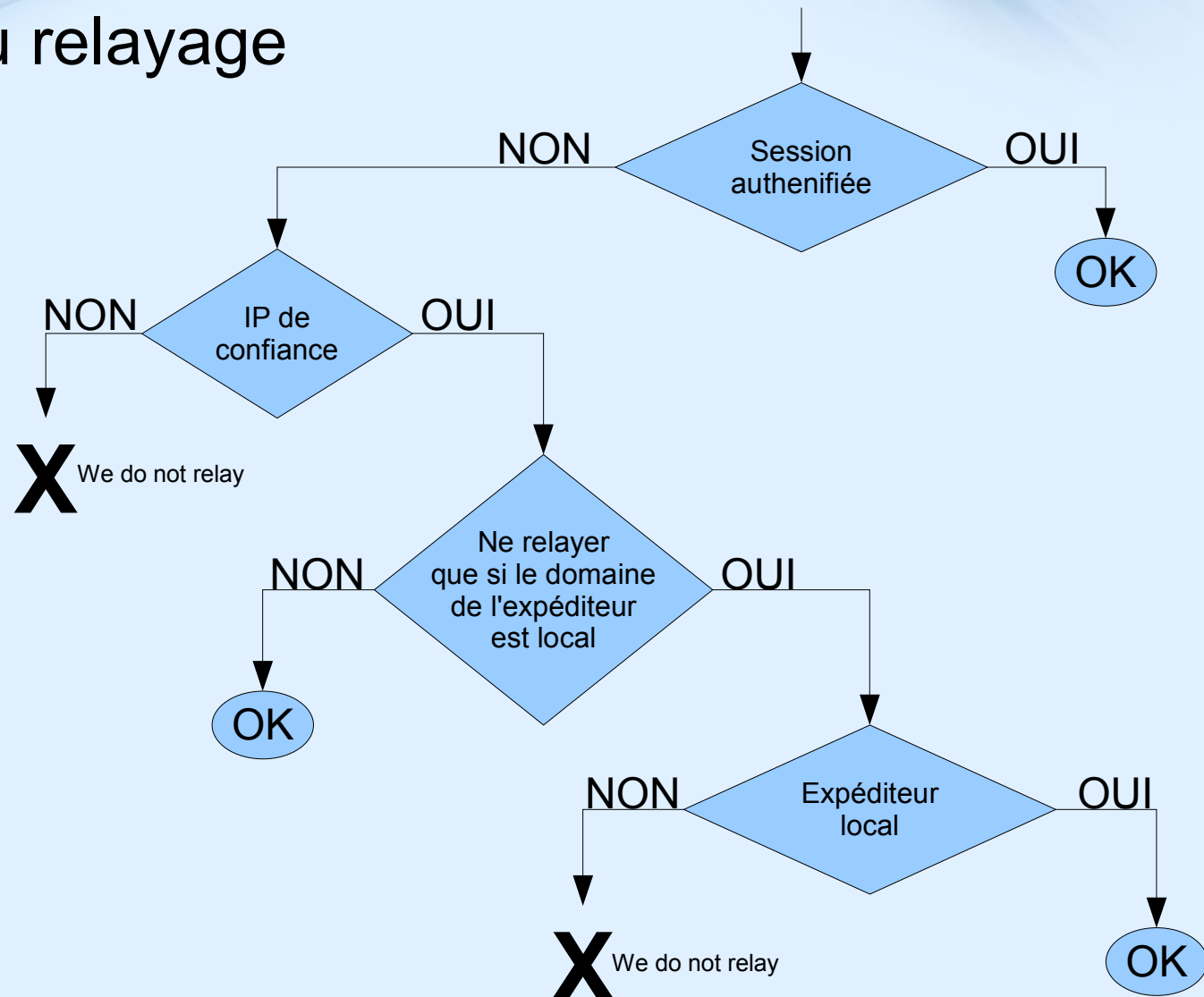
ou

<http://home2.paulschou.net/tools/xlate/>

" we do not relay "

```
222.170.127.111 [2314] 18:51:10 Connected
222.170.127.111 [2314] 18:51:10 >>> 220 mail.tassigny.darnis.com ESMTP IceWarp 10.0.0 (2009-09-21); Mon, 21 Sep 2009 18: ...
222.170.127.111 [2314] 18:51:10 <<< HELO mailer
222.170.127.111 [2314] 18:51:10 >>> 250 mail.tassigny.darnis.com Hello mailer [222.170.127.111], pleased to meet you.
222.170.127.111 [2314] 18:51:10 <<< MAIL FROM:<turbofan34@gmail.com>
222.170.127.111 [2314] 18:51:11 >>> 250 2.1.0 <turbofan34@gmail.com>... Sender ok
222.170.127.111 [2314] 18:51:11 <<< RCPT TO:<krack@greataccuratereliable.eu>
222.170.127.111 [2314] 18:51:11 >>> 550 5.7.1 <krack@greataccuratereliable.eu>... we do not relay <turbofan34@gmail.com>
222.170.127.111 [2314] 18:51:11 *** <turbofan34@gmail.com> <krack@greataccuratereliable.eu> 0 0 00:00:00 INCOMPLETE-SESSION
222.170.127.111 [2314] 18:51:11 Disconnected
```

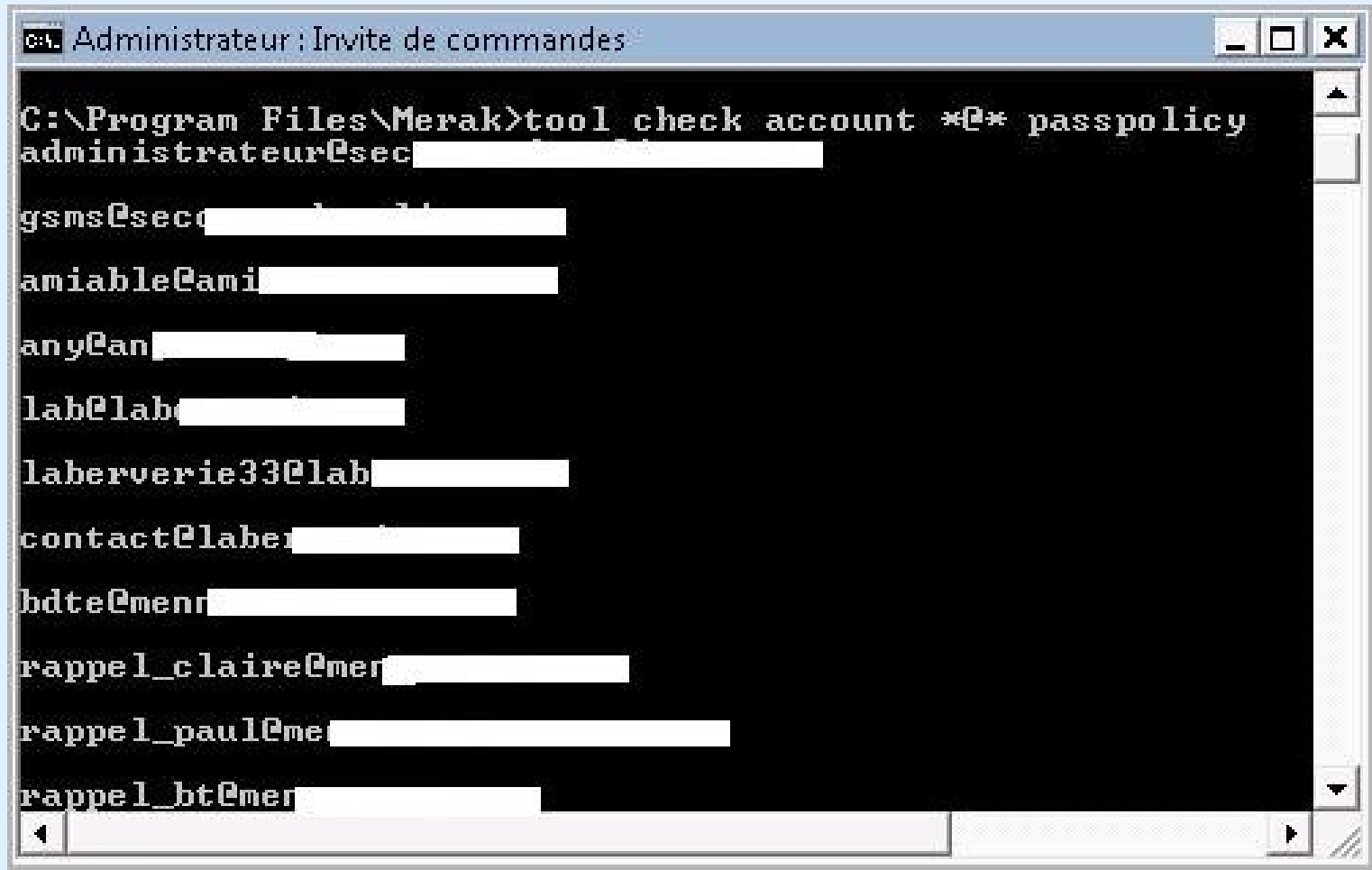
Contrôle du relayage



Un compte de domaine local doit être identifié

```
77.224.234.202 [0DA0] 10:12:47 Connected
77.224.234.202 [0DA0] 10:12:48 >>> 220 secosys.dnsalias.org ESMTP IceWarp 10.0.0 RC6; Sat, 26 Sep 2009 10:12:48 +0200
77.224.234.202 [0DA0] 10:12:48 <<< EHLO static-202-234-224-77.ipcom.comunitel.net
77.224.234.202 [0DA0] 10:12:48 >>> 250-secosys.dnsalias.org Hello static-202-234-224-77.ipcom.comunitel.net [77.224.234.202], pleased to me
77.224.234.202 [0DA0] 10:12:48 <<< MAIL FROM:<claudellecelinda@iwdemo.org> SIZE=6586
77.224.234.202 [0DA0] 10:12:48 >>> 250 2.1.0 <claudellecelinda@iwdemo.org>... Sender ok
77.224.234.202 [0DA0] 10:12:48 <<< RCPT TO:<claudellecelinda@iwdemo.org>
77.224.234.202 [0DA0] 10:12:48 >>> 550 5.7.1 <claudellecelinda@iwdemo.org> Access to <claudellecelinda@any78.org> not allowed
77.224.234.202 [0DA0] 10:12:48 <<< QUIT
77.224.234.202 [0DA0] 10:12:48 >>> 221 2.0.0 secosys.dnsalias.org closing connection
77.224.234.202 [0DA0] 10:12:48 *** <claudellecelinda@iwdemo.org> <claudellecelinda@iwdemo.org> 0 0 00:00:00 INCOMPLETE-SESSION
77.224.234.202 [0DA0] 10:12:48 Disconnected
```

Vérification des mots de passe



```
Administrateur : Invite de commandes
C:\Program Files\Merak>tool check account *@* passpolicy
administrateur@sec[redacted]
gsms@sec[redacted]
amiable@ami[redacted]
any@an[redacted]
lab@lab[redacted]
laberverie33@lab[redacted]
contact@laber[redacted]
bdte@menr[redacted]
rappel_claire@mer[redacted]
rappel_paul@me[redacted]
rappel_bt@mer[redacted]
```


" SSL côté émetteur - client "

```
SYSTEM [2028] 21:19:58 Client session Message id IDU60958 item 200910012119584388.tm$
SYSTEM [2028] 21:19:58 Client session DNS query 'secosys.dnsalias.org' 0 (0) [OK - 2]
SYSTEM [2028] 21:19:58 Client session Connecting to 'secosys.dnsalias.org'
78.114.121.81 [2028] 21:19:58 Client session Connected
78.114.121.81 [2028] 21:20:00 Client session <<< 220 secosys.dnsalias.org ESMTP IceWarp 10.0.0 RC6; Thu, 01 Oct 2009 21:19:55 +0200
78.114.121.81 [2028] 21:20:00 Client session >>> EHLO mail.tassigny.darnis.com
78.114.121.81 [2028] 21:20:00 Client session <<< 250 HELP
78.114.121.81 [2028] 21:20:00 Client session >>> STARTTLS
78.114.121.81 [2028] 21:20:00 Client session <<< 220 2.0.0 Ready to start TLS
78.114.121.81 [2028] 21:20:00 Client session SSL: Verified (0)
78.114.121.81 [2028] 21:20:00 Client session >>> EHLO mail.tassigny.darnis.com
78.114.121.81 [2028] 21:20:00 Client session <<< 250 HELP
78.114.121.81 [2028] 21:20:00 Client session >>> MAIL From:<bertrand@darnis.com> SIZE=632 TRANSID= <200910012119584388....>
78.114.121.81 [2028] 21:20:00 Client session <<< 250 2.1.0 <bertrand@darnis.com>... Sender ok
78.114.121.81 [2028] 21:20:00 Client session >>> RCPT To:<bertrand@secosys.dnsalias.org>
78.114.121.81 [2028] 21:20:00 Client session <<< 250 2.1.5 <bertrand@secosys.dnsalias.org>... Recipient ok
78.114.121.81 [2028] 21:20:00 Client session >>> DATA
78.114.121.81 [2028] 21:20:00 Client session <<< 354 Enter mail, end with "." on a line by itself
78.114.121.81 [2028] 21:20:00 Client session >>> 632 bytes (overall data transfer speed=73148148 b/s)
78.114.121.81 [2028] 21:20:14 Client session <<< 250 2.6.0 632 bytes received in 00:00:13; Message id IDU27656 accepted for delivery
78.114.121.81 [2028] 21:20:14 Client session *** <bertrand@darnis.com> <bertrand@secosys.dnsalias.org> 1 632 00:00:13 OK IDU60958
78.114.121.81 [2028] 21:20:14 Client session >>> QUIT
78.114.121.81 [2028] 21:20:14 Client session <<< 221 2.0.0 secosys.dnsalias.org closing connection
SYSTEM [2028] 21:20:14 Client session Disconnected
```

SSL côté destinataire - serveur

```
193.251.36.243 [0B44] 21:19:54 Connected
193.251.36.243 [0B44] 21:19:55 >>> 220 secosys.dnsalias.org ESMTP IceWarp 10.0.0 RC6; Thu, 01 Oct 2009 21:19:55 +0200
193.251.36.243 [0B44] 21:19:55 <<< EHLO mail.tassigny.darnis.com
193.251.36.243 [0B44] 21:19:55 >>> 250-secosys.dnsalias.org Hello mail.tassigny.darnis.com [193.251.36.243], pleased to meet you.
193.251.36.243 [0B44] 21:19:55 <<< STARTTLS
193.251.36.243 [0B44] 21:19:55 >>> 220 2.0.0 Ready to start TLS
193.251.36.243 [0B44] 21:19:55 <<< EHLO mail.tassigny.darnis.com
193.251.36.243 [0B44] 21:19:55 >>> 250-secosys.dnsalias.org Hello mail.tassigny.darnis.com [193.251.36.243], pleased to meet you.
193.251.36.243 [0B44] 21:19:55 <<< MAIL From:<bertrand@darnis.com> SIZE=632 TRANSID=<200910012119584388@darnis.com>
193.251.36.243 [0B44] 21:19:56 >>> 250 2.1.0 <bertrand@darnis.com>... Sender ok
193.251.36.243 [0B44] 21:19:56 <<< RCPT To:<bertrand@secosys.dnsalias.org>
193.251.36.243 [0B44] 21:19:56 >>> 250 2.1.5 <bertrand@secosys.dnsalias.org>... Recipient ok
193.251.36.243 [0B44] 21:19:56 <<< DATA
193.251.36.243 [0B44] 21:19:56 >>> 354 Enter mail, end with "." on a line by itself
193.251.36.243 [0B44] 21:19:56 <<< 637 bytes (overall data transfer speed=1919 b/s)
193.251.36.243 [0B44] 21:19:56 Start of mail processing
193.251.36.243 [0B44] 21:20:09 *** <bertrand@darnis.com> <bertrand@secosys.dnsalias.org> 1 632 00:00:13 OK IDU27656
193.251.36.243 [0B44] 21:20:09 >>> 250 2.6.0 632 bytes received in 00:00:13; Message id IDU27656 accepted for delivery
193.251.36.243 [0B44] 21:20:09 <<< QUIT
193.251.36.243 [0B44] 21:20:09 >>> 221 2.0.0 secosys.dnsalias.org closing connection
193.251.36.243 [0B44] 21:20:09 Disconnected
```

SSL sur la liaison IP (wireshark)

```
3.213 193.251.36.243 192.168.1.11 TCP 54055 > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1452
3.213 192.168.1.11 193.251.36.243 TCP smtp > 54055 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3.292 193.251.36.243 192.168.1.11 TCP 54055 > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
4.294 192.168.1.11 193.251.36.243 SMTP S: 220 secosys.dnsalias.org ESMTP IceWarp 10.0.0 RC6; Thu, 01 Oct 2009 21:19:55 +0200
4.375 193.251.36.243 192.168.1.11 SMTP C: EHLO mail.tassigny.darnis.com
4.377 192.168.1.11 193.251.36.243 SMTP S: 250-secosys.dnsalias.org Hello mail.tassigny.darnis.com [193.251.36.243], pleased to...
4.461 193.251.36.243 192.168.1.11 SMTP C: STARTTLS
4.462 192.168.1.11 193.251.36.243 SMTP S: 220 2.0.0 Ready to start TLS
4.542 193.251.36.243 192.168.1.11 SSLv3 Client Hello
4.543 192.168.1.11 193.251.36.243 SSLv3 Server Hello, Certificate, Server Hello Done
4.678 193.251.36.243 192.168.1.11 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4.681 192.168.1.11 193.251.36.243 SSLv3 Change Cipher Spec, Encrypted Handshake Message
4.762 193.251.36.243 192.168.1.11 SSLv3 Application Data, Application Data
4.764 192.168.1.11 193.251.36.243 SSLv3 Application Data, Application Data
4.848 193.251.36.243 192.168.1.11 SSLv3 Application Data, Application Data
4.963 192.168.1.11 193.251.36.243 TCP smtp > 54055 [ACK] Seq=1990 Ack=608 Win=64733 Len=0
5.041 192.168.1.11 193.251.36.243 SSLv3 Application Data, Application Data
5.123 193.251.36.243 192.168.1.11 SSLv3 Application Data, Application Data
5.126 192.168.1.11 193.251.36.243 SSLv3 Application Data, Application Data
5.208 193.251.36.243 192.168.1.11 SSLv3 Application Data, Application Data
5.209 192.168.1.11 193.251.36.243 SSLv3 Application Data, Application Data
5.301 193.251.36.243 192.168.1.11 SSLv3 Application Data, Application Data
5.463 192.168.1.11 193.251.36.243 TCP smtp > 54055 [ACK] Seq=2356 Ack=1486 Win=65340 Len=0
5.542 193.251.36.243 192.168.1.11 SSLv3 Application Data, Application Data
5.663 192.168.1.11 193.251.36.243 TCP smtp > 54055 [ACK] Seq=2356 Ack=1560 Win=65266 Len=0
8.558 192.168.1.11 193.251.36.243 TCP 57452 > smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
8.636 193.251.36.243 192.168.1.11 TCP smtp > 57452 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1452 WS=0
8.636 192.168.1.11 193.251.36.243 TCP 57452 > smtp [ACK] Seq=1 Ack=1 Win=66792 Len=0
8.637 192.168.1.11 193.251.36.243 TCP 57452 > smtp [FIN, ACK] Seq=1 Ack=1 Win=66792 Len=0
8.716 193.251.36.243 192.168.1.11 TCP smtp > 57452 [ACK] Seq=1 Ack=2 Win=65535 Len=0
8.717 193.251.36.243 192.168.1.11 SMTP S: 421 4.7.1 Intrusion prevention active for [78.114.121.81]
8.717 192.168.1.11 193.251.36.243 TCP 57452 > smtp [RST, ACK] Seq=2 Ack=60 Win=0 Len=0
8.718 193.251.36.243 192.168.1.11 TCP smtp > 57452 [FIN, ACK] Seq=60 Ack=2 Win=65535 Len=0
```

Firefox

Le domaine ne correspond pas



Cette connexion n'est pas certifiée

Vous avez demandé à Firefox de se connecter de manière sécurisée à **192.168.1.11**, mais nous ne pouvons pas confirmer que votre connexion est sécurisée.

Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.

Que dois-je faire ?

Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.

Sortir d'ici !

▼ Détails techniques

192.168.1.11 utilise un certificat de sécurité invalide.

Le certificat n'est valide que pour `secosys.dnsalias.org`.

(Code d'erreur : `ssl_error_bad_cert_domain`)

▼ Je comprends les risques

Si vous comprenez ce qui se passe, vous pouvez indiquer à Firefox de commencer à faire confiance à l'identification de ce site. **Même si vous avez confiance en ce site, cette erreur pourrait signifier que quelqu'un est en train de pirater votre connexion.**

N'ajoutez pas d'exception à moins que vous ne connaissiez une bonne raison pour laquelle ce site n'utilise pas d'identification certifiée.

Ajouter une exception...

Firefox

Le certificat est auto signé, expiré et le domaine ne correspond pas



Cette connexion n'est pas certifiée

Vous avez demandé à Firefox de se connecter de manière sécurisée à **192.168.1.11**, mais nous ne pouvons pas confirmer que votre connexion est sécurisée.

Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.

Que dois-je faire ?

Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.

Sortir d'ici !

▼ Détails techniques

192.168.1.11 utilise un certificat de sécurité invalide.

Le certificat n'est pas sûr car il est auto-signé.
Le certificat n'est valide que pour IceWarp Software.
Le certificat a expiré le 23/07/2005 16:00.

(Code d'erreur : sec_error_expired_issuer_certificate)

► Je comprends les risques

Internet Explorer

Le domaine ne correspond pas ou le certificat n'est pas signé par une autorité reconnue



Le DNS



<http://www.mxtoolbox.com/>

a:darnis.com

a

Type	Domain Name	IP Address	TTL
A	darnis.com	64.33.14.60	86400

Reported by [ns.dns7947.net](#) on Monday, January 01, 0001 at 3:22:54 AM

mx:darnis.com

mx

Pref	Hostname	IP Address	TTL		
5	mail.tassigny.darnis.com	193.251.36.243	86400	SMTP Test	Blacklist Check
10	mail.darnis.com	174.133.204.226	86400	SMTP Test	Blacklist Check

Reported by [ns29455.ovh.net](#) on Monday, January 01, 0001 at 3:46:31 AM

txt:darnis.com

txt

Type	Domain Name	TTL	Record
TXT	darnis.com	86400	k=rsa; n=1024; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD/YwD8hInT27Y5SBBF/cxA7cNwepsFi+LrpZoUWo8/NmY7YNJdxPgZ9RBUW46OyfDAISVvwic0BEsqgrAN4Ju8LXtVu97AUcDI3xscl/yh48gRo83R7dub5w2NVYvKtLm/9MholoVF+Spvb5YowHIMu4H3wXVbv7YGR6A7RrOzpQIDAQAB
TXT	darnis.com	86400	v=spf1 a mx ~all

Reported by [ns203149.ovh.net](#) on Monday, January 01, 0001 at 3:46:46 AM

ptr:193.251.36.243

ptr

Domain Name	IP Address
lst-amand-152-33-5-243.w193-251.abo.wanadoo.fr	193.251.36.243

Reported by [mxtoolbox.com](#) on Tuesday, October 13, 2009 at 3:47:05 AM

Architecture

